PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-291043
(43)Date of publication of application : 30.11.1990

(51)Int.Cl. G06F 15/00
G06F 15/30
G09C 1/00
H04L 9/32

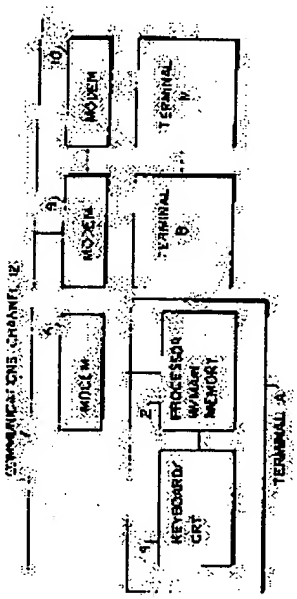
(21)Application number : 02-053483
(22)Date of filing : 05.03.1990

(71)Applicant : FISCHER ADDISON M
(72)Inventor : FISCHER ADDISON M

(30)Priority
Priority number : 89 319780 Priority date : 07.03.1989 Priority country : US

(54) METHOD FOR SIGNATURE AND CERTIFICATION IN DIGITAL SYSTEM

(57)Abstract:
PURPOSE: To enable a person, who receives a signed message together with a certificate issued by a class system, to confirm that the authority represented by a signer exactly bears the responsibility by intensifying limits and responsibilities of classes.
CONSTITUTION: After generating an ordinary text or an un-ciphered message and performing the required signature operation, each terminal transmits the message to another terminal connected to a communication channel 12. Each terminal can verify the signature of each message. Each terminal user has a public key for encryption and a private secret key for decryption related to this public key. However, he confide his encryption procedures and encryption key but doesn't decode ciphered messages neither confide the private key for decryption required for signature.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−291043

⑤Int.Cl.⁵	識別記号	庁内整理番号	㊸公開　平成2年(1990)11月30日
G 06 F 15/00	330 A	7361−5B	
15/30	340	6798−5B	
G 09 C 1/00		7343−5B	
H 04 L 9/32			
		6945−5K　H 04 L 9/00　A	

審査請求　未請求　請求項の数 51　(全40頁)

㊹発明の名称　ディジタル方式により署名および証明するための方法

㉑特　願　平2−53483
㉒出　願　平2(1990)3月5日
優先権主張　㉜1989年3月7日㉝米国(US)㉛319780

㉗発明者　アデイスン・フイツシヤー　アメリカ合衆国、フロリダ・33942、ネイプルズ、フオーテイーンス・アベニユー・サウス・60
㉑出願人　アデイスン・フイツシヤー　アメリカ合衆国、フロリダ・33942、ネイプルズ、フオーテイーンス・アベニユー・サウス・60
㉔代理人　弁理士　川口　義雄　外2名

明　細　書

1．発明の名称

ディジタル方式により署名および証明するための方法

2．特許請求の範囲

(1) 複数の端末装置を通信チャネルに連結した通信システムであって、前記通信チャネルを通じて前記端末装置の使用者が私的メッセージを交換できるように構成されており、前記使用者の各々がパブリックキーと関連プライベートキーを有している通信システムにおいて、伝達されるメッセージにディジタル方式により署名および証明するための改良された方法であって、

ディジタルメッセージを作成する段階と、

前記メッセージにディジタル署名する段階と、

前記メッセージにおいて前記メッセージの署名者に付与された権限を特定する段階とを含んで成るディジタル方式により署名および証明するための方法。

(2) 前記特定段階が、委任証明書において付与される権限を定める段階を含んでいる請求項1に記載の方法。

(3) 前記特定段階が、メッセージの署名者に対して証明書を証明者に代わって取り消す権限および証明者に代わって権限を副委任する権限を付与する段階を含んでいる請求項2に記載の方法。

(4) 前記特定段階が、メッセージの署名者の機密保護レベルまたは機密委任レベルを定める段階を含んでいる請求項1に記載の方法。

(5) 委任証明書によって、署名者の署名に付帯させねばならない連帯署名要件を定める請求項3に記載の方法。

(6) 使用者の署名を承認したことを示す第3者によるディジタル署名を要求することによって、連帯署名要件を定める請求項5に記載の方法。

(7) 前記連帯署名要件を定める段階が、ディジタ

ルメッセージに登場させる必要のある少なくともう1つのディジタル署名を特定することによって合同署名要件を定める段階を含んでいる請求項5に記載の方法。

(8) 伝達されるメッセージのハッシュ値を伝達される厳密なビット対ビットデータに基いて作成する段階と、

メッセージの印字版の真偽を検証するように構成された補助ハッシュ値を生成する段階と、

両方のハッシュ値をディジタル署名の一部として組入れる段階とをさらに含んで成る請求項1に記載の方法。

(9) 通信チャネルを通じてメッセージを交換するための通信システムにおいて、伝達されるメッセージにディジタル式に署名するための方法であって、

伝達されるメッセージのハッシュ値を、伝達さ

れる厳密なビット対ビットデータに基づいて生成する段階と、

メッセージの印字版の真偽を検証するように構成された補助ハッシュ値を生成する段階と、

両方のハッシュ値をディジタル署名の一部として組入れる段階とを含んで成る方法。

(10)前記補助ハッシュ値の生成段階が、

メッセージの少なくとも第1部分の中の全部のタブ文字をブランクに変更する段階を含んでいる請求項9に記載の方法。

(11)前記補助ハッシュ値の生成段階が、

メッセージの少なくとも第1部分の中の、印字可能な文字とならない制御文字を削除する段階を含んでいる請求項9に記載の方法。

(12)前記補助ハッシュ値の生成段階が、

メッセージの少なくとも第1部分の中の結果的には1つまたはそれ以上のブランクが印字される

ことになる情報をブランクに変更する段階を含んでいる請求項9に記載の方法。

(13)前記補助ハッシュ値の生成段階が、

メッセージの少なくとも第1部分の中の導入ブランクおよび後続ブランクを削除する段階と、

メッセージの中の完全にブランクである行を削除する段階を含んでいる請求項9に記載の方法。

(14)前記補助ハッシュ値の生成段階が、

メッセージの中の複数個連続するブランクを1つのブランクに変更する段階を含んでいる請求項9に記載の方法。

(15)前記補助ハッシュ値の生成段階が、

メッセージを1行毎に処理し、処理済みの行情報に制御情報を追加して行の終わりを区切る段階を含んでいる請求項9に記載の方法。

(16)前記補助ハッシュ値を用いて前記メッセージを含む印字文書の真偽を検証する段階をさらに含

んでいる請求項9に記載の方法。

(17)前記真偽を検証する段階が、

前記メッセージの主要部を入力する段階と、

前記入力したメッセージ主要部に関してホワイトスペースハッシュ値を計算する段階と、

前記文書の前記印字版からディジタル署名を入力する段階と、

前記ディジタル署名からのホワイトスペースハッシュ値と、前記計算により得たホワイトスペースハッシュ値とを比較する段階とを含んでいる請求項16に記載の方法。

(18)前記ディジタル署名を指定証明書と共に生成する段階と、

前記メッセージを含む文書の真偽を検証する段階とをさらに含んで成り、該検証段階が、

印字文書上のディジタル署名と前記ディジタル署名に関連するシールとを入力する段階と、

前記ディジタル署名のハッシュを計算して第1数値を生成する段階と、

前記シールのハッシュを署名者のパブリックキーを用いて処理して第2数値を生成する段階と、

第1数値と第2数値を比較して該文書が指定証明書と共に署名されているかどうかを判定する段階とを含んでいる請求項9に記載の方法。

(19)通信チャネルを通じてメッセージ交換するための通信システムにおいて、伝達されるメッセージにディジタル式に署名するための装置であって、

伝達されるメッセージのハッシュ値を伝達される厳密なビット対ビットデータに基づいて生成するための手段と、

メッセージの印字版の真偽を検証するように構成された補助ハッシュ値を生成するための手段と、

前記両方のハッシュ値をディジタル署名の一部として組入れるための手段とを含んで成る装置。

請求項19に記載の装置。

(20)前記補助ハッシュ値の生成手段が、

メッセージの中の印字可能な文字とならない制御文字を削除するための手段を含んでいる請求項19に記載の装置。

(21)前記補助ハッシュ値の生成手段が、

結果的には1つまたはそれ以上のブランクが印字されることになる情報をブランクに変更するための手段を含んでいる請求項19に記載の装置。

(22)前記補助ハッシュ値の生成手段が、

メッセージ中の導入ブランクおよび後続ブランクを削除するための手段と、

メッセージの中の完全にブランクである行を削除するための手段とを含んでいる請求項19に記載の装置。

(23)前記補助ハッシュ値の生成手段が、

メッセージの中の複数個連続するブランクを1つのブランクに変更するための手段を含んでいる

請求項19に記載の装置。

(24)前記補助ハッシュ値を用いて前記メッセージを含む印字文書の真偽を検証するための手段をさらに含んでいる請求項19に記載の装置。

(25)前記真偽を検証するための手段が、

前記メッセージの主要部を入力するための手段と、

前記入力したメッセージ主要部に関してホワイトスペースハッシュ値を計算するための手段と、

前記文書の前記印字版からディジタル署名を入力するための手段と、

前記ディジタル署名からのホワイトスペースハッシュ値と、前記計算して得たホワイトスペースハッシュ値とを比較するための手段とを含んでいる請求項24に記載の装置。

(26)前記メッセージを含む文書の真偽を検証して、指定証明書と共に前記ディジタル署名を作成する

ための手段と、

印字文書上のディジタル署名および前記署名の表示のシールを入力するための手段と、

前記ディジタル署名のハッシュを計算して第1数値を生成するための手段と、

前記シールのハッシュを署名者のパブリックキーを用いて処理して第2数値を生成するための手段と、

第1数値と第2数値を比較して、該文書が指定証明書と共に署名されているかどうかを判定するための手段とをさらに含んでいる請求項19に記載の装置。

(27)通信チャネルを通じてメッセージ交換するための通信システムにおいて、前記メッセージにディジタル式に署名する方法であって、

複数の関係はあるがそれぞれ別個のメッセージ部分を含むディジタルパッケージを組立てる段階

と、

署名すべき個別メッセージ部分のリストを生成する段階と、

少なくとも前記個別メッセージ部分のリストのディジタル表示を署名者のプライベートキーを用いて処理することにより、複数の個別文書をパッケージとして組織し、処理した後署名する段階とを含んで成る方法。

(28)伝達する複数の個別メッセージ部分に関するハッシュ値を計算する段階と、

ハッシュ値を前記個別メッセージ部分のリストに記憶させる段階とをさらに含んでいる請求項27に記載の方法。

(29)前記処理段階が、

少なくとも前記関連メッセージ部分のリストまたは該メッセージ部分のハッシュを反映するハッシュ値を計算する段階と、

前記ハッシュ値を用いて署名用シールを生成する段階とを含んでいる請求項27に記載の方法。

(30)前記個別メッセージ部分の少なくとも1つに関して補助ハッシュ値を計算する段階と、

前記ハッシュ値と前記補助ハッシュ値の両方を前記ディジタルパッケージ用ディジタル署名の一部として組入れる段階とを含んでいる請求項28に記載の方法。

(31)前記補助ハッシュ値がホワイトスペース正規化ハッシュ値である請求項30に記載の方法。

(32)前記ディジタルパッケージの組立て段階が前記パッケージの署名の定義を生成する段階を含んでいる請求項27に記載の方法。

(33)前記ディジタルパッケージの組立て段階が、前記パッケージの中に少なくとも1つのディジタル証明書部分を含ませることにより受け手側で当該署名が有効であり然るべき権限を与えられてい

るかどうかを判定できるようにする段階を含んでいる請求項27に記載の方法。

(34)前記組立て段階が、伝達すべき添え状のディジタル表示と関連の同封書状とを組立てる段階を含んでいる請求項27に記載の方法。

(35)前記組立て段階が、添え状のディジタル表示と少なくとも1つのディジタルデータファイルを組立てる段階を含んでいる請求項27に記載の方法。

(36)前記ディジタルパッケージを受信した時点でその真偽を検証する段階を含んでおり、その段階が、

前記関係メッセージ部分の少なくとも複数部分に関してハッシュ値を計算する段階と、

計算で得たハッシュ値と関係メッセージ部分リストの中の対応値とを比較する段階とを含んでいる請求項28に記載の方法。

(37)ディジタルパッケージを受信した時点でその

パッケージの真偽を検証する段階をさらに含んでおり、前記検証段階が、パッケージの署名に実際に使用されているディジタル署名がパッケージに有効なディジタル署名を表すものかどうかを検証する段階を含んでいる請求項28に記載の方法。

(38)前記ディジタル署名の検証段階が、指定されたプライベートキーを用いて、受け取ったメッセージ部分の各々に受け取ったディジタル署名に示された順序で署名が行なわれているかどうかを判定する段階を含んでいる請求項37に記載の方法。

(39)パッケージのディジタル署名のみを用いて少なくとも1つのメッセージ部分を個別に検証する段階を含んでいる請求項27に記載の方法。

(40)通信チャネルを介してメッセージ交換するための通信システムにおいて、前記メッセージにディジタル式に署名するための装置であって、

複数の関係はあるが別個のメッセージ部分を含

むディジタルパッケージを組立てるための手段と、

署名すべき個別メッセージ部分のリストを作成するための手段と、

少なくとも前記個別メッセージ部分のリストのディジタル表示を署名者のプライベートキーを用いて処理することにより、複数の個別文書をパッケージとして組織し、処理した後署名できるようにするための手段とを含んで成る装置。

(41)少なくとも伝達すべき複数の個別メッセージ部分に関してハッシュ値を計算するための手段と、

前記個別メッセージ部分のリストにハッシュ値を記憶させるための手段とをさらに含んでいる請求項40に記載の装置。

(42)前記処理手段が、

少なくとも前記関係メッセージ部分のリストまたはそれらのハッシュ値を反映するハッシュ値を計算するための手段と、署名用シールを生成する

ための手段とを含んでいる請求項40に記載の装置。

(43)前記個別メッセージ部分の少なくとも1つに関して補助ハッシュ値を計算するための手段と、

ハッシュ値および前記補助ハッシュ値を前記ディジタルパッケージ用ディジタル署名の一部として組入れるための手段とを含んでいる請求項41に記載の装置。

(44)前記補助ハッシュ値がホワイトスペース正規化ハッシュ値である請求項43に記載の装置。

(45)前記ディジタルパッケージ組立て手段が前記パッケージ用の署名の定義を作成するための手段を含んでいる請求項40に記載の装置。

(46)前記ディジタルパッケージが前記パッケージの中に少なくとも1つのディジタル証明書部分を含むことにより、受け手側で当該署名が有効であり然るべき権限を付与されているかどうかを判定できるように構成されている請求項40に記載の装

置。

(47)前記ディジタルパッケージが伝達すべき添え状および関連する同封書状のディジタル表示を含んでいる請求項40に記載の方法。

(48)前記ディジタルパッケージが添え状のディジタル表示と少なくとも1つのディジタルデータファイルを含んでいる請求項40に記載の装置。

(49)ディジタルパッケージを受信した時点で該パッケージの真偽を検証するための手段と、

前記関係メッセージ部分の少なくとも複数部分に関してハッシュ値を計算するための手段と、

計算したハッシュ値と関係メッセージ部分のリストの中の対応数値とを比較するための手段とを含んでいる請求項41に記載の装置。

(50)ディジタルパッケージの受信時に該パッケージの真偽を検証するための手段をさらに含んでおり、前記検証手段がパッケージの署名に実際に使

用されているディジタル署名が該パッケージに有効なディジタル署名を表すものかどうかを検証するための手段を含んでいる請求項40に記載の装置。

(51)ディジタル署名検証手段が、指定されたプライベートキーを用いて受信メッセージ部分の各々に受信したディジタル署名に示された順序で署名したかどうかを検証するための手段を含んでいる請求項50に記載の装置。

3．発明の詳細な説明

本出願は、1988年2月12日出願の特許出願第155,467号の一部継続出願である。

[産業上の利用分野]

本発明は暗号通信システムおよびその方法に係る。より詳細には、本発明はディジタル署名を改良された方法で証明して少なくともディジタルメッセージの送り手に関連して身分、職権、および責任のレベルを示すパブリックキー式または署名

式の暗号システムに係る。

［発明の背景と概要］

電子郵便システム、電子振替決済システム等の急速な発達によって、低防備な通信チャネルを通じて伝達されるデータの保護に関する関心が高まっている。安全性の無いチャネルを通じて通信されるメッセージのプライバシーおよび信頼性を確保するために広く使用されているのが暗号システムである。

従来の暗号システムでは、暗号化方法を用いて通常の文章によるメッセージを理解できないメッセージに変換した後、解読方法を用いて暗号化メッセージを復号して元の形のメッセージに戻すということを行なう。

従来の暗号署名および認証システムは一般に「一方向性」ハッシング機能を用いて通常の文章によるメッセージを理解し難い形に変換する。こ

こで言う「ハッシング」機能とは、あるデータの集合体に適用すると、それより小形でしかも処理し易いデータの集合体を作り出せる機能のことである。

ハッシング機能の重要な特徴の1つとして、「一方向性」機能であるということがある。ハッシングが「一方向性」機能であるため、ある意味を含むデータを計算によって与えるのは容易であるが、ハッシュ値を与えられてもその中に含まれる意味を判断することもそのハッシュとして特定の値を有するデータを作り出すことも不可能なはずである。実際の用途では、元のデータ集合体にハッシング機能を適用して獲得された数値は、元のデータを示す模造不可能な独特の指紋となる。元のデータに何らかの変更が成されると、変更されたデータのハッシュも異なるものとなる。

従来の暗号システムでは、2進化情報を暗号と

称される理解不能な形とし、キーと称される2進符号を用いた暗号化と解読動作を連続して行なうアルゴリズムを用いて元の形に解読して戻す。例えば、1977年に規格基準局がデータ暗号化基準（ＤＥＳ）と呼ばれるブロック暗号アルゴリズムを認可している（Data Encryption Standard, FIPS PUB 46, 規格基準局, 1977年1月15日）。

ＤＥＳでは、ＤＥＳアルゴリズムをキーと共に用いて2進化データを暗号として保護する。暗号化したコンピュータデータを使用する権限を持つ使用者グループの各メンバーがデータの暗号化に使用したキーを保有し、データの使用時にはこれを必要とする。メンバーが共通して保有するこのキーを用いてグループ内の他のメンバーから暗号の形で送られて来たデータを解読する。

特定用途に合わせて選択されたキーによって、ＤＥＳアルゴリズムを用いてのデータを暗号化し

た結果が独特のものとなる。異なるキーを選択することによって、一定の入力用に作成される暗号が異なるものとなる。使用権利の無い者が暗号文を受け取った場合、ＤＥＳアルゴリズムを知っていても秘密のキーを知らなければアルゴリズムによって元のデータを引き出すことはできない。

このようにデータを暗号として保護できるか否かは、データの暗号化および解読に使用されるキーに対する保護に係っている。従来の暗号システムのほとんどがそうであるように、ＤＥＳシステムを最終的に保護できるか否かも、暗号キーの秘密を保てるかどうかに係っている。ＤＥＳシステムによるキーは64個の2進数字を含み、そのうち56個がＤＥＳアルゴリズムによってキーの有意数字として直接使用されるのに対し、8個の数字はエラー検出に使用される。

このような従来の暗号システムでは、メッセー

ジの送り手と受け手にシークレットキーを配布するに際して、何らかの安全な方法を取る必要がある。既存の暗号システムの主な問題点の１つとして、送り手と受け手が第三者にはキーが入手できないように１つのキーを交換しなければならないことがある。

しかもこのようなキーの交換は、メッセージの交換前に例えば私設の配達員や書留郵便等を用いてキーを送付する方法で行なわれることが多い。このようなキーの配布方法は、必要とされる機密保護は達成できても時間がかかる上に費用も高くなるのが普通である。送り手と受け手にとって私的なメッセージ交換が必要なのは１回限りであれば、メッセージ交換を私設配達員や書留郵便を用いて行なえば良いのであり、暗号通信は不要となる。また私的な通信を緊急に行ないたい場合、専用キーの配布にかかる時間による遅れは容認し難

いものとなる。

パブリックキーによる暗号システムは従来の暗号システムに見られたキー配布問題の多くを解決するものである。パブリックキーによる暗号システムでは、暗号化と解読の相互関係を絶って、暗号化用キーと解読用キーを別個のものとする。すなわち、暗号化キー毎にそれと対応する解読キーがあり、この解読キーは暗号化キーと異なるものである。暗号化キーが分かったとしても解読キーが算出されるおそれはない。

パブリックキーシステムを用いると、シークレットキーの伝達を行なわずに私的通信を行なうことができる。パブリックキーシステムでは暗号化キーと解読キーを対で生成することを必要とする。使用者全員のための暗号化キーは配布しても公表しても良く、通信を希望する人は自分のメッセージを宛先の使用者のパブリックキーの下で暗号化

するだけで良い。

解読用シークレットキーを保有している宛先ユーザだけが送信されて来たメッセージを解読することができる。暗号化キーが露顕しても解読キーについては何ら役立つようなことは開示されない。すなわち解読キーを知っている人しかメッセージの解読を行なえないのである。Rivest et alの米国特許第4,405,829 号に開示のＲＳＡ暗号システムは、パブリックキー暗号システムの実施のための方法論の一例を示したものである。

パブリックキー暗号システム等の主な問題点は、受信したメッセージの送り手が実際にメッセージに記名された人物かどうかを確認しなければならない点にある。「ディジタル署名」を用いた周知の認証方法によって、使用者は自分のシークレットキーを用いて「メッセージに署名する」ことができるようになり、受け手側または第三者は斜作

者のパブリックキーを用いて署名を確認することができる。この方法については、米国特許第4,405,829 号等を参照されたい。

このようなディジタル署名の出現により、現在ではどのようなディジタルメッセージにでも署名をつけることによって受け手側がそのメッセージが実際に送信されたものであり、偽物でないことを確認できるようになっている。このような確認は、特許第4,405,829 号に記載されているように「パブリックキー」とディジタル署名法を用いて行なうが、この方法を以後ＲＳＡ技術と呼ぶ。ＲＳＡ以外の方法を用いたパブリックキーおよび署名技術も存在しており、Fiat-Shamir 法、Ong-Schnorr-Shamir法その他の無知識立証技術から派生した方法がいくつかある。これらの方法にはＲＳＡのように守秘性のあるものは無いが、ディジタル署名は行なえる。本発明は特定のパブリッ

クキーや署名技術に限定されないものである。

使用者は公けのアクセスし得るファイルにパブリックキーをファイルした後、メッセージを送信する前にメッセージまたはメッセージのハッシュを使用者のプライベートキーを用いて「解読」（または「署名」）することによってメッセージにディジタル署名することができる。メッセージの受け手は送り手の暗号化用パブリックキーを用いて暗号化することによってメッセージまたは署名を検証することができる。このように、ディジタル署名法は通常の暗号化方法の逆になり、メッセージをまず解読した後に暗号化する。使用者の暗号化用パブリックキーを持っていれば誰でもメッセージまたは署名を読むことができるが、解読用のシークレットキーを持っている送り手側しかメッセージまたは署名の作成はできない。

一般にディジタル署名は署名が計算された時点

でのメッセージの完全性を受け手に対して保証するものである。しかし署名者の真偽については、ディジタルメッセージへの署名に用いたパブリックキーが実際に送り手であるとされる者に属するものである程度にしか保証されない。この問題はディジタル署名の使用が普及するに従ってますます重要なものになって来ており、様々な通信者（おそらく他の点では相互に未知の人々）が中央にキープされている「登録簿」（またはその他の手段）を通じて相互のパブリックキーを通じて相互のパブリックキーを入手しているのが現状である。

従って、特定のパブリックキーが特定の個人によって実際に作り出されたものであることを保証するパブリックキー式暗号システムにも重大な問題が存在すると言える。この問題に取組んだ公知方法の1つとして、政府機関等の信頼のおける公

共機関に各パブリックキーとそれの真の創作者であると主張する人とが確実に結び付くようにしてもらおうとする試みがある。

信頼し得る公共機関が権利主張者のパブリックキーと権利主張者の氏名（当該機関の意に沿うように厳密なもの）を内容とするディジタルメッセージを作成し、当該機関の代表者が当該機関自身の署名でディジタルメッセージに署名する。証明書と呼ばれることも多いこのディジタルメッセージが権利主張者自身のディジタル署名と共に送付される。権利主張者のメッセージを受け取った人は、機関のパブリックキー（機関署名の検証を可能にする）を認知することを条件に、またその受け手の当該機関に対する信用の度合いに応じて署名を使用することができる。

証明書は信頼のおける機関が署名した短かいメッセージであり、その中で証明されているパブリ

ックキーおよび該パブリックキーの所有者（作成者）の身分に関する説明を明瞭にあるいは暗黙に含んでいるものであると考えることができる。このように解釈した場合、"C" が "A" のための証明書を与えたとすると、受け手である "B" は、"B" が "C" を信用することを条件に、また "B" が "A" のパブリックキーに関する "C" の証明を保有していることを条件として、"A" のパブリックキーの使用を信用することができる。

従来の通信システムでは、伝達された証明書にメッセージの送り手の持つ信用の度合いまたは責任の程度を示すものは何もない。証明書は単に、そこに明示されている信用のある機関が送り手のパブリックキーをその人物のものであると認知したことを証明するものにすぎない。

パブリックキーシステムは、様々な使用者のパブリックキーを公けにして私的通信を成立し易く

するように運用することを目的として設計されたものであるが、パブリックキーシステムの使用希望者の数が増えるに従って公開されたパブリックキーの数もやがては、パブリックキーの発行機関が公開されたパブリックキーを有する人が本当にその所有者であると主張している人であることを適正に保証できない規模になるものと考えられる。そして例えばゼネラル・モータース・コーポレイション等の大企業の社長の名で公開登録簿にパブリックキーを掲載する事態が生じるかもしれない。この場合の個人は、ゼネラル・モータース社長宛ての私的メッセージを受信したり、表面的には人格としての社長に属する署名を作成し得る地位にある人となる。

また、Fiat-Shamir アルゴリズムのように、完全なパブリックキーの機能を必要としないディジタル署名の作成方法もある。パブリックキー式暗

ことにより、両当事者が事実上相互に未知の場合をも含めてより多様な業務に使用し得るものとする。

本発明は証明に関連するいろいろな属性を特定する能力を提供するという利点を有する。これらの属性は単に個人の正確な身分を保証するだけでなく、証明者が被証明者に与えた権限や制約（多様な状況における）を実際に特定するものである。

例えば、本発明によると会社が特定のパブリックキーを特定の従業員が使用していることを証明できるようになるだけでなく、その雇用関係において当該個人に対して会社が与えている権限を明確にすると共に会社を代表してパブリックキーを使用していることを明示することも可能になる。

認可される権限の種類や等級に制限はない。本発明では、証明を受ける者（被証明者）に権限が付与されたことを示す方法でディジタル署名の証

号システムと言う時、それは署名システムを反映するものであるとも解釈するべきである。パブリックキーの解読と言う時は、それは署名の作成を概括的に言っているのであり、暗号化と言う時は署名の検証について言っているととるべきである。

本発明は、ディジタル署名証明の能力を拡大することによって、パブリックキー保有者の身元確認に関してパブリックキーまたは署名による暗号システムの持つ問題に取り組むものである。これに関して、後述するように多重レベルの証明法を用いると同時に証明しようとする署名をした個人の「権限」も示す証明方法を採用している。ここで用いる「権限」という用語は、ディジタル署名または証明者の使用を通じて付与された権力、支配力、委任、職権委任の責任または拘束を広く示すものである。

本発明はパブリックキー式暗号の性能を高める

明を行なう。証明者は証明書を作成する際に、証明を受けるパブリックキーを固定する欄、および被証明者の名前、身分等を含む特別メッセージを作成する。証明者の作成する証明書にはさらに付与されている権限および課せられている制限や保障条項も含まれる。この中には、例えば被証明者に対する金額的限度や被証明者に対して与えられている信用の程度のように証明者に関係する問題を反映した情報が含まれる。証明書はまた、被証明者に対して課されている連帯署名要件も特定することもできる。本発明に包含されるより実際的な種類の権限および／または拘束を要約すると下記のようになる。

証明書には被証明従業員が特定のディジタル署名を使用して委任し得る金額を盛込むことができる。このような制限条件は、ディジタルネットワークを通じて電子決済される機会が多くなるに従

って、ますます重要性を帯びるものと考えられる。この制限内容は証明書に「内蔵」されるため、受け手は誰でも例えばディジタル署名されている購入注文書が有効であるかどうか即座に判断できるようになる。

本発明はまた、特定の証明パブリックキーを使用する場合は必ずディジタル「連帯署名」を必要とするようにできる。「連帯署名」という用語を、ここでは「合同」署名と「副署名」の何れも含めて使用する。ここで言う合同署名とは、同じ「対象物」（例えば購入注文書）に直接成される署名であるのに対し、副署名とは別の署名に添付される署名である。原則的には合同署名は任意の順序で「並記」できるが、副署名は既存の署名を特定的に「批准」するものである。従って本発明のディジタル署名証明方法および装置は、証明および署名に階層を設けていると言える。連帯署名要件

提供する。合同署名に対する要件は、例えば金銭の振替を行なったり送金許可を得る場合に特に有効である。この目的を達成するために、本発明の証明書は（パブリックキーと被証明者の名前およびその他の欄に加えて）必要とされる合同署名の数および資格を有する合同署名者の身分に関する指示事項を反映するように構成される。従って、合同署名を行なうことを要求されるその他のパブリックキー保有者の各人に対する明確なリストを証明書の中に含ませることもできる。このようにして、受け手側は、送り手側の証明書の許可を得て署名されているデータが他の何人かの特定署名者による署名を必要とすることを知らされる。従って受け手側は、証明書の中の各署名に存在するパブリックキーを比較するだけで、他の合同署名および副署名を検証することができる。本発明はまた、他の証明書を参照するなど、これ以外の連

に関しては、副署名および合同署名の要件を各ディジタル証明毎に参照することにより、これまでは少なくとも一方の側が物質的に企業官僚主義を打破しない限り行なわれることの少なかった電子業務処理を可能にする。これによって企業は例えば経費の許可をとる（その他適当と思われる機密を要する目的）ために多くの署名を要する現在の慣行をまねて実施することができるようになるであろう。この要件は本発明のディジタル証明書の中に内蔵されているため、受け手側には（1つまたはそれ以上の）連帯署名が必要な時が明らかになり、受け手（または受け手側のソフトウェア）は必要とされる適当な連帯署名が存在しているかどうかを判断することができる。

本発明はさらに、証明用の合同署名がさらに必要であることをディジタルメッセージの受け手に明らかにするようなディジタル署名の証明方法も

署要件表示方法も含んでいる。他のパブリックキー保有者に関する表示は、明確にしても良いし（ここに記載するようなリストを用いて）、あるいはその他何らかの機能または所属を特定する方法であいまいにしても良い。この機能または所属は各連帯署名者の証明書の中に表示しても良い。

本発明は証明書の中に「機密委任」レベルを組入れることも包含するものである。これによって例えば軍（またはその他の安全保障関連機関）はその証明書の中に機密保持を織込むことができるようになる。この特徴によって署名入りメッセージを作成した人物の確実な機密保持レベルを確認することが可能になる。

これと逆に、またおそらくはより重要な特徴として、ディジタルメッセージを送る際に付加的な点検レベルを提供し得る点がある。すなわちメッセージを暗号化する時に（受け手側のパブリック

キー、従って受け手側の証明書も要するプロセス）、本発明を具体化したコンピュータシステムでは全ての受け手が然るべき機密保護上の認可を得て機密情報を含む特定メッセージを受信するように保証することが可能になる。

さらに、本発明は受け手側に副証明を行なう信用レベルを与えるようなディジタル署名の証明方法を提供する。このようにして責任に関する信用レベルが中央の信頼できるソースから流される。

本発明の例示的実施態様では、証明者は、証明書に記名された使用者を証明者が知っておりかつ関連パブリックキーの使用を認証されていることを証明者が保証することを示す信用レベルに、所定のディジタルコードを割当てることができる。但し、このディジタルコードによって使用者（「被証明者」）が証明者に代わってそれ以上の身分証明や証明を行なう権限を与えられるもので

限を示す署名を明確に含むものとなる。このような署名付きメッセージの受け手は、署名付きメッセージと証明書の全階級とを合わせて分析した結果に基いて直ちに業務処理を行なえるように送り手の権限を検証することができる。

本発明は大型システムまたはシステム群を階級的に管理する能力も提供する。またそれを行なうに当たって、制御性を良くし、間違い、変造、ごまかし、悪意の混乱等を抑止できるようにする。

本発明によって作成される証明書は単なる身分証明だけでなく、金銭上の権限も含めて権限、制約、制限をも伝えるものであるため、極めて重要なものであるため、証明行為は厳正に実施し注意深く管理しなければならない。大組織（または組織群）においては、全員の身分を中央で確認するのが困難になる（権限については言うまでもない）。また常時移動があるため、従業員の地位の

はない。別の方法として、パブリックキーの使用者が証明者に代わって他の人物の身元を厳正に確認することを委託されており、また（おそらくは）使用者が適当と考えるようにこの権限を委任することをも委託されていることを示すコードを含むその他のディジタルコードを有する証明書を証明者が発行することもできる。

本発明はさらに、多くの方法（例えば異なる証明者による証明書等）で証明される使用者のパブリックキーも提供する。本発明は適当な証明書を使用者が署名したメセージの一部として含むことも包含する。このような証明書には、署名者の証明者のための証明書や証明者の証明者のための証明書から関係者全員による信託を受けた所定の証明書（または相互委託した1組の共同証明書）まで含まれる。この場合、各々の署名付きメッセージが証明書の序列または階級、および送り手の権

変更に伴なって証明書の再発行が必要になる。本発明はこれらの要件を満足するために、配分式階級管理を組込んでいる。

本発明は階級から階級への制限と責任を強化することにより、（階級制によって出された）証明書と共に署名されたメッセージを受けた人がその署名者の代表する権限が厳正に責任を負うことを確認することができる。

これを達成するのは下記の方法による：

1)各証明書の一部として、認可されている権能、権限および制限事項に関するステートメント（コンピュータによって容易にチェックでき、場合によっては人による確認が容易に行なえる形式で）を含ませる。

2)各証明書において、証明者が階級制に準じてさらに認可され得るであろう機能および権限を規定する（多少でもあれば）。

3)認可している権限が重要であったり、価値の高いものであったり、慎重を要するものである場合、この中にはおそらくはさらに次のレベルに権限を委譲する権能や、金銭その他の慎重を要する資産を委任する権能が含まれるであろうが、複数の署名（連帯署名）を必要とするという条件を規定することができる。この時、連帯署名について明確に表示しても良いし（別の証明書やパブリックキーを挙げて）、あるいはあいまいに表示しても良い（証明書またはパブリックキーの種類を特定したり、何らかの抽象的な組分けや同定方法によって）。

これによって抑制と均衡の機能、相互決定機能、慎重を要する機能行使時の自己規制機能が強化される。また、汚職の発生する可能性を少なくすることによってシステム全体の完全性が高まり、例え汚職でなくても損害の発生を抑制する。共謀に

よる悪事の危険性は、必要とする連帯署名の数を増やすことによって確実に低下させることができる。

4)大組織においては、パブリックキーのもつ私的側面が場合によっては弱点となる（おそらくはパブリックキー所有者の不注意にもより）ため、ネットワークを通じて取消し通知を出す必要性も生じ得る。

従来技術では、証明書の作成者（証明者）が証明書を取消しするしか実際的方法としてはなかった。そうでなければ悪意またはいたずらによってにせの取消し通知が出され、罪の無い所有者の証明書を誤って無効にすることで大混乱を生じるおそれがあるためである。

本発明を使用すると、普及した方法で取消し手続きを管理することができ、証明書を実際に作成した人が必ず取消しを実行する人である必要がな

くなる。これによって「審査」力を安全に統制することができ、しかも証明書を定義しその正確さを保証する人々が常時注意している必要もない。

本発明はさらに、添え状関連同封書状、関連グラフィックファイル等の複数の対象物に、それらの対象物を個々に検証できるような方法で一括して署名することができ、しかも各対象物と全体との関係を表示し得る方法も提供する。これら全部の対象物に関係するデータの集合体（おそらくは各対象物と制御情報とのハッシュ）を順序付けリストに集める。次にこの順序付けリストを対象物としてみなし、これに署名するか、あるいはリストのハッシュに署名する。このリストは、署名者が関連対象物だけでなく全体の中でのそれらが占める位置をも個人的に認知したことを示すものである。従ってこの順序付けリストの中の各要素をハッシングアルゴリズムによって処理する（より

コンパクトなリストを作り出すように）結果、前署名ハッシュ値のリストとなる。次に前署名ハッシュリストを解読（署名）サイクルにかけると、結果的に署名者の署名となる。これを以後シールと呼ぶことにするが、シールは後に詳しく説明するように署名パケットの一部となるものである。

本発明はさらに、コンピュータ検証できると同時に将来用紙に印字したものから再入力して再確認を要する場合にも再検証できるような署名を生成する文書ディジタル署名方法も提供する。この目的を達成するために、文書形式のコンピュータメッセージのディジタル署名に2つのハッシュ値を用いる。使用するハッシュ値のうち1つめのものはファイルの中の厳密なビット対ビットデータに関連するものであり、これがコンピュータによって読取り可能な形でアクセスできる限り、正確な原文書の検証が可能になる。

本発明はまた2つめの補助ハッシュ値も使用する。第2ハッシュ値に使用されるデータが「ホワイトスペース正規化」される以外はファイルの中の同一データに関して取られる値である。ホワイトスペース正規化を行なうことによって、将来のある時点で、プリントアウトしたものから必要に応じてデータを再入力することができるが、この時、どのような種類の印字不能、知覚不能な制御文字が原本に存在していてもそれについて心配する必要がない。

用途によっては、パブリックキー、証明書およびディジタル署名が別個ではあるがいくらか重なり合った機能を行なうように設計する場合もあることを認識する必要がある。これに関連して、「パブリック」キーの中にここでは「証明書」と呼んでいるものの一局面を含ませることもできよう。それと逆に証明書の方をその一部としてパブ

リックキーを含む構成とすることもできる。同様に、証明書および／またはパブリックキーのいくらかまたは一部を署名の一部とすることもできる。この可能性については、別の証明書に権限を与える署名を行なう時に特に留意する必要がある。以下の詳細な説明の中に示す特定実施例は本発明を限定するものではない。

以下の本発明の好適実施態様についての説明を添付図面を参照しながら読むことによって、これまでに述べたものも含めて本発明の特長がより良く理解されよう。

第1図は本発明と共に使用し得る通信システムの1例を示す構成図である。このシステムの端末A，B，…N間の通信を行なう通信チャネル12は無防備である。この通信チャネル12を例えば電話回線とする。端末A，B，…Nを例えば従来のキーボード／ブラウン管4とプロセッサ（主記憶機

能付き）2を連結したIBM製パーソナルコンピュータとするが、これに限定されるものではない。各端末A，B，…Nは従来形IBM製パーソナルコンピュータ用通信盤（不図示）も含んでおり、これらを従来形モデム6，8，10にそれぞれ接続すると、端末はメッセージの送受を行なうことができる。

それぞれの端末が通常文または暗号化していないメッセージの作成と必要とされる署名動作の実行を行なった後、通信チャネル12（または通信チャネル12に接続された通信網（不図示））に接続されている他の端末にメッセージを伝達することができる。また、端末A，B，…Nのそれぞれが各メッセージ毎に署名の検証を行なうことができる。

端末使用者（パブリックキーに関連して上述した通り）各自が暗号化用パブリックキーとそれに

関連する解読用プライベートシークレットキーを保有する。第1図に示したパブリックキー式暗号システムでは、端末使用者各自が他の端末使用者のメッセージ暗号化の一般的方法について承知している。また、端末使用者各自が端末の暗号化手続きで暗号化メッセージの生成に使用する暗号化キーについても承知している。

但し、端末使用者は自分の暗号化手続きと暗号化キーを明らかにしても、暗号化したメッセージを解読したり、署名を行なうのに必要な解読用プライベートキーは明らかにしない。また、暗号化キーを知っていてもそれを用いて解読用キーを算出することは不可能である。

端末使用者は私的メッセージの伝達の他に、伝達メッセージにディジタル署名を行なうこともできる。端末使用者がメッセージ伝達の前に自分の解読用プライベートキーを用いてメッセージを解

読する方法でメッセージにディジタル署名することができる。受け手はメッセージを受けると送り手の暗号化用パブリックキーを使用してメッセージを読むことができる。このようにして受け手側ではそのメッセージを作成したのが解読用シークレットキーの保有者に間違いないことを確認することができる。これが署名入りメッセージの受け手に対してそのメッセージが送り手によって作成されたものであることを証明する証拠となる。本発明と共に使用し得るディジタル署名方法の一例について、米国特許第4,405,829 号に詳細に開示されている。

本発明によるディジタル証明方法の改良について詳しく説明する前に、例えば電子郵便のパブリックキー式暗号法における第1図の概略的動作について説明することにする。まず、端末Aの使用者がゼネラルモータース社のコンピュータ自動化

設計課の比較的地位の低い課長であり、他の州にあるコンピュータソフトウェア販売会社からソフトウェアパッケージを購入しようとしていると仮定する。コンピュータソフトウェア販売会社はその店舗に端末Nと関連モデム10を所有している。

端末Aのゼネラルモータース社の課長は注文品目と注文品の送り先の他、標準的な購入注文書で必要とされるその他の項目を明示した電子購入注文書を作成する。ここでは電子購入注文書を例にとっているが、署名にどのようなパブリックキー方式を採用していてもそれを用いて処理するのに適当な方法で表現できるデータの集合であれば、任意のデータ集合体を伝達できることを認識する必要がある。以下のより詳細な説明では、このようなデータ集合体、例えばコンピュータデータファイルを総括的に「対象物」と呼ぶことにする。

端末Aの使用者であるゼネラルモータース社課

長は、後述するような伝達メッセージに添付する証明書により委任された権利の下に購入注文書にディジタル署名する。まず課長のディジタル署名について言えば、署名対象物の少なくとも一部分に個人的に所有している署名キーを適用することによって「署名」することができる。対象物の画像（または後に詳細するような対象物のダイジェストまたはハッシュとして知られるより簡潔な形にしたもの）にシークレットキーを用いて署名することによって、パブリックキーを使用し得る者であれば誰でもがこの結果を「暗号化」（すなわち逆転）してそれを対象物（または計算し直してハッシュまたは数字の形にしたもの）と比較することが可能になる。パブリックキーの所有者しかシークレットキーを用いてこの動作を実行できなかったはずであるから、それによってパブリックキーの所有者がメッセージに署名をしたことが確

認される。Fiat-Shamir のような異なる署名方式には「暗号化」以外の方法が適当である場合もあることが注目される。

本発明によると、ディジタル署名に加えて署名者の身分と該署名者に対して与えられている権限とを特定する有効証明書を少なくとも1通付着させる。この証明書は、特定パブリックキーの使用者の身分と、該使用者より高レベルの権限を有する当事者から該使用者に対して与えられている権限とを特定する特別な対象物またはメッセージとみなすこともできる。

証明書が有効であるためには、1通またはそれ以上の他の有効証明書と関連のあるプライベートキーによる署名が必要である。これらを以後、当該証明書の先行証明書と呼ぶことにする。先行証明書にも満足すべき制限事項および／または制約事項（おそらくは連帯署名等）が付随するかもし

れない。これらの先行証明書は各々が署名者に対してかかる署名を行なう権限および／または本例では購入注文書を発行する権限を認めるものでなければならない。これらの先行証明書にも満足すべき制限事項および／または制約事項（おそらくは連帯署名等）が付随するかもしれない。それぞれの先行証明書にそのまた先行証明書がある場合が生じるのである。

本発明の一実施態様では、全証明書の最終的先行証明書として仮に米国標準局のような世界的に知られた権威のある機関による証明書を利用し、これを超証明書と称する。世界的な信用と著名度を要するのは超証明書のみである。超証明書は署名を必要としない。また超証明書は広く公表、配布されるものと想定される。複数の超証明書が存在する場合があり、また複数の超証明書が所要の連帯署名に関して相互に参照し合う場合もある。

複数の超証明書の使用が重要になる用途は多い。それぞれの超証明書も尊重されるであろうが、当然どの加盟会社も汚職の危険性に関心を払う必要があるためである。各組織の「最高レベル」の証明書に個々に参画する全員に対して各々が「非の打ちどころのない」複数の超証明書を要求することによって、現実の危険性も予測される危険性も大幅に減らすことができる。さらに、組織が適当と認めれば組織毎に連帯署名要件を確立することができるため、組織毎にその組織内での汚職の危険性を抑制することができる。

先の例に戻ると、最終的に端末Ａから端末Ｎのコンピュータソフトウェア販売会社にメッセージが送られると、受け手側では後に詳述する方法でゼネラルモータース社課長の署名を検証する。また、メッセージ証明書および先行証明書にその他の署名が揃っていることも確認し、それによって

端末Ｎのソフトウェア販売会社ではその取引が有効であり、完全に認可されたものであるとの保証を得る。ここで認識しておかねばならないのは、購入品目を出荷する前にこのような保証を得ることが非常に重要であり、電子式振替決済の場合はおそらくさらに重要になるということである。

端末Ａの使用者から送られたメッセージを受けた相手方（この相手方が端末Ｎの最終的なメッセージの受け手であるか、ゼネラルモータースのような会社組織内の他の当事者であるかを問わず）は、Ａの署名と端末Ａの使用者の行使した権利の検証ならびに有効性確認を行なうことができる。このような確認を行なえるのは、元の購入注文書と共に証明書の有効性確認の上での完全な階層順位も伝達されており、最終的受け手として申し込みのあった取引が本物であり然るべき認可を得たものであることを確信できるためである。

例えばゼネラルモータース社から出された主要取引にもっと包括的に焦点を当てる場合、まず上述の最終的証明者、すなわち超証明者に焦点を当てるのが有効である。この場合、ゼネラルモータースとゼネラルモータースと取引きしようとする相手方またはその他の形でパブリックキー式暗号システムに参加している関係者とは、最初に例えば仮に米国標準局および／または国内最大級の銀行の何れかのような世界的に認知されている権威のある機関に接近を図ることができる。このシステムの法人その他の参加者は１組のパブリックキー（その法人の重役会の決定に基いて使用する権利を与えられたもの）と共に十分な裏付けのための書類および証拠品を超証明書に提示する。これらのパブリックキーは主としてゼネラルモータース社内の職員の証明用にゼネラルモータース社内で使用される「高レベル」のキーである。超証明

者（または各超証明者）はゼネラルモータース社に対し、供給されたパブリックキーは何れもゼネラルモータース社の正当なる権限によって自身の使用のために作成されたものである旨の証明を配布する。実際には、超証明者が証明しているのはそれぞれのキーを使用する当事者は実際にゼネラルモータース社と関連があるということである。超証明者の証明の中には、登録されたパブリックキーの使用者が正にゼネラルモータース社と関連があることを示す埋め込み文が含まれていると言える。例えば、ゼネラルモータース社が3つの「高レベル」キーの証明を受け、これらを例えば副社長、財務担当役員、安全保障担当役員のような会社役員に保持させることを決定したとする。ゼネラルモータース社の要請があれば、3枚の証明書のそれぞれが、他の2人のパブリックキーが連帯署名を要すると表示するように構成すること

もできる。

従って、超証明者から一旦最高レベルの証明書を受けると、ゼネラルモータース社内の複数の役員が次に下位のレベルの証明書に合同署名しなければならなくなる場合がある。一般には、これらの高レベルのゼネラルモータースの証明書の各々が相互に連帯署名者を要するとして参照し合うことになろう。従ってこのレベルでは、会社役員の中で単独で何かを完全に認可し得る人はいなくなるのである。これは3つの証明書の各々の中に特に同定された他社の署名を要するという条件が埋込まれているためである。次にこれら3人の役員が他のゼネラルモータース社従業員のためのパブリックキーを作成してこれに署名する。このパブリックキーは各従業員が持つべき権利、責任および制限事項定めるものである。これらの証明書の何れかを使用者Aに帰属させるか、あるいはこれ

が使用者Aの証明書の先行証明書となる。

これら3つの高レベル証明書は好適には対面確認するか、あるいはその他の人的な検証、確認の後に端末Bの使用者の証明書にディジタル署名することができる。各必要署名を行なった後、副社長、財務担当役員、安全保障担当役員による証明書の署名とそれぞれの3通の証明書、およびそれらの証明書の超証明者によるそれぞれの署名が端末Bのゼネラルモータース社長のもとへ最終的に戻され、現在進行中の用途、今の例では端末Aの使用者の副証明のために記憶される。このように、記憶された署名メッセージは端末Aの使用者の身分とその権限を検証する証明書および署名の序列または階層順位を明白に内容として含んだものになる。

証明序列の中の当事者Bが当事者Aに対する権限委譲証明書を作成する場合、その証明書はAの身分と共にAの暗号化用パブリック署名／キーも含んだものとなる。また、その証明書はBがAに対して認可したい権利、権能および制限条件も表示する。この証明書を与えることによってBはAの身分と権限の両方に対する責任を明確にとることになるのである。

Aに対するBの証明書によって、後述するようにこの証明書を用いる時にAのとる行為に連帯署名する必要のある他の当事者の特定も行なうことができる。連帯署名は合同署名の形をとる場合と副署名の形をとる場合がある。また、当事者BはAに対する証明書においてAによって行なわれる副証明をBがどこまで認めるかを規定することができる。

本発明の例示的実施態様によると、証明者から被証明者に与えられる信用の度合いが所定のディジタルコードで証明書に特定される。メッセージ

の受け手はこの信用度を、証明されているパブリックキーの使用に関して被証明者に付与されている権限および証明者のとる責任を示す指針として用いる。

例えば、信用レベルのみを信用レベル値０，１，２，３で示すことができる。

信用レベル０は、証明者は証明のパブリックキーが証明書に記名された個人に属するものであることを証明するが、被証明者の作成する証明書の厳正さに関して責任をとるものではないということを示す。要するにこれは証明者が「この証明書に記名された使用者を存じており関連するパブリックキーの使用を証明されていることを保証する…が、彼が私に代わって証明を行なうことを委任はしない」と言明していることになる。

信用レベル１は被証明者に対し、証明者に代わって信用レベル０の証明を行なう権限を与えるも

のである。本質的には、これは証明者が、「このパブリックキーの使用者を存じており、彼／彼女が私に代わって他の人の身分証明を正しく行なうことを委任する。またこの身分証明に関して私が責任を負うが、私はこの者に対して、身分証明される人々が信用に値するかどうかを判断することは委任していない」と言明していることになる。

信用レベル２は被証明者に対し、証明者に代わってレベル０，１，２の証明を行なう権限を与えるものである。本質的にはこれは証明者が、「このパブリックキーの使用者を存じており、彼／彼女が私に代わって他の者の身分証明を正しく行なうことを委任する。また、彼らが適当と認めた場合にこの権限を委任する権限も与える。彼らまたは彼らによって任命された然るべき権限を有する代理人または然るべく任命された代理人そのまた代理人によって成された証明の責任は私が負う」

と言明していることになる。

信用レベル３はそのパブリックキーと証明書が確立されると共に周知となっており（おそらくは広域的マスメディア広告により）、しかもその的確さが世界的に高く評価されている最終的な認証明者に専用のレベルである。この証明者は証明するパブリックキーの所有者である実体の身分証明を正確に行なうことにのみ責任を負う。パブリックキーの使用に関しては全く責任を取らない。

証明者は自分の作成した他の証明書を無効にする権限を他の者に与えることもできる。一般には、どの証明者でも自分の参加した証明書を無効化または取消しできると仮定される。また、一般には被証明者も自分自身の証明書についてその信用が失われたとする正当な理由があればこれを取消すことができると仮定される。さらに、本発明は「全く誰でもが」既存の証明書に署名を付け加え

ることができないように動作する（そのような場合、取消す権限を付与されているように見えるかもしれないからである）。本発明は証明書の中に元の署名者のパブリックキーのハッシュまたは証明書の他、該証明書に署名することも許可されている他の当事者に関する表示（一般的にはパブリックキーのハッシュまたは証明書の何れかであるが、場合により他の抽象的証明書または証明者群のコード）を組入れる。その他の署名者は被証明者に対して定められた全ての権利を然るべく委任することを要求される場合がある。本発明は証明者の誰もが個人的に完全には所有することのできないような権力の委任を行なう証明書の作成をその一目的とする。

証明者にとっては、（選ばれた）他の使用者が自らのために「警察」権を行使できるようにするのが有利である。従ってこの例示的実施態様では、

証明者によって付与される「警察」権（すなわち解消権）を証明書が反映し得る方法を採用している。本実施態様では、取消し権と先に定義した「身分証明」の信用レベルとは別個のものとして区別する。本発明の１つの方法では、証明者が次の４種類の取消し権の１つを付与することができる。

０：使用者は、証明者の管理下にある他の証明書を取消す特別な資格を付与されない。

１：使用者は証明者の取消せるものであれば任意の証明書を取消しすることができる（それに伴う拘束条件も受ける）。

２：１と同様であるが、使用者が自分に付与された取消し権を付与できる（但し、使用者はさらに義務を負わせる権利を委任することはできない）点で異なる。

３：２と同様であるが、使用者が（完全に）権

限委任する権能を完全に委任できる点で異なる。

別の方法として、このような取消し権を信用レベルと関連させても良い。一例として、信用レベル１または信用レベル２に関連する権限の中に証明書の取消し権も含ませることができる。

このように取消し行為を管理する権利を配分することによって、証明書作成者が必ず取消し者である必要がなくなる。また、別の方法として証明書の取消し権のみに関わる別個の信用レベルを規定しても良い。

さらに、高度の機密を要する企業情報や軍事情報を扱う組織内で使用する場合、証明書の中に機密委任許可レベルも定めることができる。これによって証明書は署名メッセージを認可した人物の正確な機密保護レベルを特定することができる。

さらに、１回の証明毎に金額限度、すなわち、被証明者が取扱いを認められている最高金額を特

定することもできる。この金額限度は、証明者が自分の取扱い許可額を超えての委任をすることのないように、証明者自身の証明書の限度を超えてはならないのはもちろんである。受け手側が組になった証明書を受け取るとこのような制限が容易に実施される。

本発明のディジタル署名および証明方法について詳しく説明する前に、まずいくつかの用語について定義するのが有効であろう。上で述べたように、「対象物」という用語は署名および／または暗号化にどのようなパブリックキー方式が用いられていてもその方式で処理するのに適するように最終的に表現することのできるデータ集合体を説明するのに包括的に使用される用語である。「対象物」という用語は購入注文書や小切手、現金振替や証明書のような「一次」対象物にも、また「二次」対象物、すなわち別の署名にも適用する

ことができる。

本発明では処理効率を向上するための方法として一般に関数を対象物に適用し、全体として小型化されてコンパクトな、より処理し易い対象物、すなわち一般には数十個以上のビットから成るサイズ固定のビットストリングとする。このような関数が対象物のハッシュまたはダイジェストと呼ばれるものである。但し、このような関数が必ず必要なわけではなく、対象物そのものを含めてその他「独特な」対象物表現法を用いても良い。

ハッシュまたはダイジェストの一例として、暗号ブロック連鎖モード（ＣＢＣ）を用いたデータ暗号化基準（ＤＥＳ）により対象物の画像を処理して獲得される出力が挙げられる。処理は２種類のＤＥＳキー（どちらも一定の公開されて一般に知られているキー）を用いて行なうことができる。その後、最終的な出力連鎖値を何らかの方法で、

おそらくは排他的論理和演算を用いて連結または併合し、ダイジェストまたはハッシュ値を構成する数十個以上のビットとする。"Square-mod-n"として知られる別のハッシュ値についてX.509認証草案に記載されている。

ダイジェストまたはハッシングアルゴリズムの重要な特徴の1つに、対象物のダイジェストを計算するのが容易であるが同等のダイジェストで異なる対象物または変更された対象物を構築することができないことがある。実用的には何れの場合でもダイジェストが元の対象物の偽造不可能な独自指紋となる。元の対象物が何らかの形で変更された場合、ダイジェストも異なるものとなる。換言すれば、実際の用途では元の対象物をよりコンパクトに表現したものがその元の対象物に独自のものとなるのである。理想的にはハッシュからは、メッセージの中に含まれる特定のデータ値に関し

て何らかも明らかにならないようにするべきである。例示的実施態様で使用されるハッシュは少なくとも128ビットを有するものである。

次に第2図に移ると、データの流れと署名の作成方法が示されている。署名法は任意のコンピュータファイルや書状、電子購入注文書等のような一般的対象物だけでなく、署名や証明書のような特殊化された対象物にも適用される。

第2図に全体的に示されているように、それぞれのディジタル署名には署名を行なうパブリックキーの証明が付帯する。証明書には、第5図に関連して詳しく説明するように1人またはそれ以上の上位権限を有する人（すなわち直系の証明者）によって署名され、原署名者の身分を証明すると共に、原署名者に付与されている権限の程度を特定する。

本発明によると、原署名者は1通以上の証明書

を有することができ、いろいろなレベルの権限に関して証明書を使い分けることができる。それぞれの証明書毎に金額限度、信用レベル、合同署名要件および副署名要件を含めた制限事項および要件が異なっている。

特定の対象物に署名する際に用いる署名／証明書を適宜選択するのは署名者の義務である。例えば購入注文書の場合、単なる照会状とは異なる種類の権限（従って異なる証明書）が必要になる。そのため証明書が署名者だけでなく署名者の権限のレベルも同定する点で伝達メッセージの非常に重要な部分となるのである。

第2図に示すように、使用者は署名を行なう際に対象物20（例えば購入注文書とする）を使用し、対象物の種類22を特定する。例えば、対象物の種類の欄に対するドキュメンテーションによって、対象物が購入注文書データファイルであることが

表示される。場合によっては対象物の種類の欄22が対象物が別の署名または証明書であることを表示することもある。24に示されるように、署名の日付も同定される。

注記欄26を用いて、例えば署名に制限条件を設けたり、その他の注記を付け加えるドキュメンテーションを行なう。署名者は対象物の自分の署名が一定期間のみ有効である旨をここに表示することができる。さらに特定の取引、例えば購入注文書に関して何か注釈をつけたいことがあれば注記データとして付け加えることができる。

やはり署名の中に組込まれるものとして原署名者の証明書28がある。この証明書は原署名者のパブリックキー30の他に第5図に関連して詳述するような多数の欄を含んでいる。上記のようにパブリックキー式署名方式はパブリックキー30と第2図の32に示す関連プライベートキーを使用するこ

とが必要である。

対象物の欄20（例えば購入注文書データ）、対象物の種類の欄22、署名日付欄24、注記欄26、署名者の証明書欄28が34でハッシングアルゴリズムを介して処理効率を高めるようにハッシュされる。さらに各欄44,22,24,26,28が署名パケット42に組込まれて署名記録の一部となる。対象物欄20をパケット42に組込む前に、これにもハッシングアルゴリズム44を適用してよりコンパクトな形にする。

これまでに述べた欄にハッシングアルゴリズム34を適用すると、その結果36に示す前署名ハッシュが得られる。次にこの前署名ハッシュ36を署名者のプライベートキー32を用いる解読（署名）サイクル38にかけることにより、署名者の署名が獲得される。これを以後シール40と呼ぶことにする。シール40は他の項目20（または20のハッシュである40）,22,24,26,28と共に最終的な署名パケット

とするシール40（署名パケットと共に伝達されたもの）に対して解読（検証）作業52を実施することによって、前署名ハッシュ54を得る。受け手はこの前署名ハッシュを署名者と同じ方法で再計算し、この値と署名者の署名の解読（検証）結果とを比較する。

ブロック56に示すように、50と54の2つの値が等しくなければ、受け手側はこの署名を有効として受け入れることはできない。意図的であるか否かを問わず、対象物および／または署名が署名された後に何らかの方法で変更されたか改ざんされたことに間違いないからである。このような検証段階を踏むことにより、受け手側はディジタル信号が指定されたパブリックキーと一致するかどうかを判断する。

このようにして対象物とそのシールを処理することにより、対象物がパブリックキーの所有者が

42となる。

この署名が関連対象物と共に伝達されると、受け手側はそれによって該対象物が署名されたままの完全な状態であることを確認することができる。また、十分な証明書も含まれていれば、受け手側は署名者の正当な身分と署名者が証明書の連鎖の中で与えられている権限を確認することができる。

次に第3図を参照すると、この図は第2図に従って構築された署名パケット42を含む伝達メッセージを受けた側が署名の検証を行なう方法を示している。第3図に示すように、受け手は署名パケット42と関連欄44,22,24,26,28を使用し、第2図でこれらの欄に適用したのと同じハッシングアルゴリズムを適用することによって前署名ハッシュ50を得る。

次に受け手側は署名者の証明書28と共に送られて来た暗号化パブリックキーを用い、検証しよう

署名した時点でのデータと同一であることを確認する。これが全体的な確認プロセスの第1段階となる。

確認プロセスのその他の段階はパブリックキーが付帯証明書の中で指定された人物に属するものであること、またその人物が証明書に明記された権限を有することを確認するものである。この検証プロセスは例えその対象物が別の署名や証明書であっても全ての対象物にあまねく適用される。確認プロセスを遂行する際、受け手側は署名に関連する各証明書を分析して、各証明書に対してその署名およびこれらの委任署名の先行証明書を介して然るべき権限が付与されているかどうかを判断する。

1つの対象物に1つ以上の署名が伴う場合がある。このような連帯署名は合同署名か副署名の何れかの範疇に入るものである。合同署名とは対象

物に異なる当事者によって成されたもう１つの署名にすぎず、その署名プロセスは第２図に関連して説明した最初の署名の作成に使用されたプロセスと何ら変りはない。

副署名とは署名の署名である。すなわち、Ａが対象物に署名した場合、この署名そのものを対象物と考えることができる。そこでＣがＡの署名に副署名すると、Ｃの署名している対象物は元の対象物ではなく、Ａの署名そのものということになる。従って副署名は副署名の対象となる署名の後でしか行なうことはできず、根本的な対象物とＡが該対象物に署名したという事実の両方を承認（または少なくとも認知）したことを反映する。このメカニズムによって、下位レベルで成された約束事をそれぞれ１つ高いレベルで承認して行くという権限の連鎖を強化することができる。このシステムの独自な特徴の１つとして、Ａがこの署

名と関連させる証明書が、Ａの署名に他の特定の合同署名または副署名を付随させることを事実上要する点にある。

次に第４図の副署名の作成方法に移ると、まずＡは第２図に関連して詳しく述べた手順に従って63において一次対象物60に署名する。この一次対象物60は購入注文書やその他の約定書であっても良いし、一次対象物の他の署名の副署名であっても良い。

第２図に関連して説明したように、Ａが対象物に署名するプロセスに他の当事者がＡの署名に署名する段階も含ませても良い。従って、Ａの証明書62は65において、Ａの署名が有効であるためには（すなわち有効確認されるためには）、例えばＣの特定証明書Ｙを用いたＣによる副署名が必要であることを明確に規定する。

Ａが対象物に署名した後、Ａの署名パケット66

が一次対象物および全ての関連署名並びに証明書と共にＣに送られ、ＡからＣにＣの副署名64が要請される。資料を受け取ったＣは既存の署名証明書全部と一次対象物を検査し、全て承認できるものであればＡの署名に署名する決定を68で行なうことになる。Ａの署名は本来一次対象物を反映するものであり、Ｃの署名は本来Ａの署名を反映するものであるため、Ｃは本質的に「Ａの署名の下の行に署名した」ことになる。

Ｃが68においてＡの署名を承認する決定をすると、第２図で詳細に示した署名作成プロセスを再び実行するが、この場合の対象物はＡの署名となる。すなわち、Ａの署名を対象物として（対象物の種類を72において署名と指定して）、副署名の日付74、Ｃの副署名の注記76、Ｃの証明書78をハッシングアルゴリズム80に適用することによって、前署名ハッシュ82を得る。同時にこれらの欄につ

いても署名パケット42に関して述べたのと同じように（ハッシングアルゴリズム69を署名対象物に適用した状態で）副署名パケット88に挿入する。

前署名ハッシュ82とＣのシークレットキー92を署名動作84に適用して副署名シール86を生成する。この副署名シールが第２図の署名パケット42の作成方法に関連して先に説明したのと厳密に同じように副署名パケット88の一部となる。

署名を行なうためにＣが使用しなければならない証明書“Ｙ”が明確に規定されたものであるため（Ａが署名に使用した証明書において）、Ｃもまた“Ｙ”によって特定された連帯署名義務を果し、Ｃ自身の付け加えた署名を含むパケット全体を他の当事者に転送してさらに連帯署名（合同署名または副署名の何れか）を求めることが必要になる場合がある。このような回帰的署名収集プロセスは、少なくとも一次対象物に最初に署名した

一当事者の全ての連帯署名要件が完全に満足されるまで継続される。

次に一当事者が他者に対する委任証明書を作成する方法について見ると、BがAに対する委任証明書を作成する時、Aの身分に関する明細とAが自分自身用に生成した暗号化パブリックキーとを結合することが注目される。また、BはBがAに対して付与したい権限の権能と制限事項も特定する。証明書に署名することによって、BはAの身分と権限に関する責任を明確にとることになる。

本発明によると、BはAが該証明を用いる時に取る行為に連帯署名することを要求される他の署名者を特定することができる。上述のように、Bはさらに A に対する証明書の中でBが認めるAによる副証明の程度も定めることができる。

その他にも多くの制限条件および拘束条件がBから課される場合がある。例えばBは、Aの証明

書を受け取った人がBの意図している金額の限度を確実に認識できるように金額制限を課すことができる。証明書作成プロセスは後述するように署名を伴うため、連帯署名の使用は証明行為の委任にも及ぶ。例えば、副証明行為の委任を特定の複数連帯署名者が関わった場合に限って許可するように証明書を構成することができる。これによって権限の階層制の中に抑制と均衡を取り入れることにより、署名を受け取る側からも、またこの署名を使用する権利を与える側からも非常な信頼を得ながら組織および制度間の境界を超えて電子式ディジタル署名を使用することが可能になる。

当事者Bが当事者Aのための証明書を作成する方法を示したのが第5図である。100 に示すように、Aが従来のパブリックキー式署名システムによりパブリックキーとプライベートキーの組を作成し、パブリックキーをB 102 に供給する。証明

のためAから与えられたパブリックキーを受け取ったBは、そのパブリックキーが実際にAによって生成されたものであり、Aを装った何者かによるものでないことを確認することが必要である。そのため、Aによって生成されたパブリックキーを対面方式で提供するのが望ましい。

Aの証明書に署名する際に用いる自分自身の証明書を選択したBは、106 において証明書108 を関連パブリックキー110 と共に用いて新しい証明書の署名112 を作成する。第2図と同様に、署名は対象物（Aの証明書116)と証明書（Bの証明書108)を用いて作成される。Bのシークレットプライベートキーを用いて新証明書116 の署名112 が作成され、Bの署名の署名パケット114 がAの新証明書パケットの一部となる。

Bによって特定されたAに関する情報を用いて構成されたAに対する証明書に焦点を当てると、

Bは回線103 を介してAから提供されたAのパブリックキーの「パブリック」な面を利用して証明書を構成する。Bはまた A の正式名、Aの肩書き、その他住所、電話番号等の重要項目を明示する。また、将来Aの証明書の検討を要する人がいれば誰でも入手できるようになる証明に注記を加えておくこともできる。

Bはさらに証明書の失効日も指示することになろう。この日付はこの日以降Aは当該証明書を使用してはならないという日付を表すものである。Bはまた証明書の中にBの組織内部での内部識別コードを表すAの口座番号を表示することもできる。

さらにBは証明書の中で金額的限度を設けることができる。金銭上の権限または信用の限度とB自身の証明書の限度とを突合せることにより、Bが委任する権限を与えられている以上の権限を委

任していないかどうかを確認することができる。これと同じ関係が将来の受け手によっても彼らの確認プロセスの一環として検証される。

上述のように、BはAによって成される副証明に関してBが負おうとしている責任の程度も定める。この欄はB自身の証明書に与えられている信用レベルとの両立性が必要である。Bに対して付与された信用レベルとBによって付与される信用レベルとの関係は、将来の受け手が彼らに呈示された証明書の階級を確認する時に必ず確認される関係の1つである。上述のように、信用レベルの中の1つまたはそれ以上が証明書を取消す関連権利を有している場合がある。また別の方法として証明書取消し権利のための信用レベルを別個に設けても良い。また、上で示したように、機密保護レベル欄を用いて証明書の中に機密委任レベルを組入れることが可能である。

Bは Aの証明書に連帯署名要件を挿入するが、その中でAが新証明書を使用する際にいくつの、またどのような種類の連帯署名をAの署名に付帯させる必要があるかを特定する。上述のように連帯署名は合同署名および／または副署名の形をとる。副署名は証明書の使用を承認したことを示すものであり、その承認の後には必然的に関連署名が続く。合同署名の順序は任意で良いが、必ずしも他の署名の承認を反映するものではなく、共通する対象物を承認（または認識）したことを示すものにすぎない。

連帯署名要件は証明書の中にいろいろな方法で特定することができる。1つの方法として、有効合同署名者リストまたは有効副署名者リストを彼らのパブリックキーまたは証明書の同定によって明確に定める方法がある。各リストと関連して、受け手側が該署名が十分に承認されていることを

認めるために最低限必要な関連署名の数を特定するが、この数は1から始まってあらゆる数が考えられる。合同署名リストは他のパブリックキーまたは特定証明書の組の中の各々のハッシュ値のベクトルとすることができる。新証明書を使用する場合、これらのキーのうち特定された最小数のキーがAによって署名された対象物に対して成された他の証明書に登場しなければならない。これが無い場合、受け手はAの署名を有効としてはならない。

副署名リストはこの証明書の許可の下に成された署名に署名する際に使用しなければならない他のパブリックキー証明書のハッシュ値のベクトルとすることができる。証明書（パブリックキーではなく）を参照することによって、それ自身がさらに合同署名または副署名を要する特定証明書の使用が可能になる。ここに登場する証明書を適宜

に選択することによって、組織が満足するレベルがどの程度であれ、そのレベルの副署名要件の階層制を作り出すことができる各範疇から特定数の連帯署名者が必要とされる。この数は例えば0，1，2または3、あるいは全員と全候補者からある少数までの範囲とすることができる。

連帯署名者候補をここに説明するようなリストとして明確に示しても良いし、あるいは各連帯署名者候補の証明書の中に指示される何らかの資格または権能の明細を特定することによってあいまいに示しても良い。

Bはさらに、BをAの証明書の一次保証人として同定した証明書の中に自分自身のパブリックキーを組入れる。Aの証明書の作成者として、BはAの証明書を取消す権限を有するものと考えられる。BはまたAの証明書に署名していろいろな種類の権利をAに付与し得る他の当事者を指定する

こともできる。

その他の欄が証明書に含まれる場合もある。例えば、証明書が最初に作成された時点を反映する現在の日付と時間を含ませることができる。第5図に示すように、完全な証明書はAに対する証明書116とAの証明書に対するBの署名の署名パケット114とを含む証明書パケットから成る。

Bの署名とそれを確認する全ての階層的証明書および署名がAによって保持され、Aが自分の証明書を使用する際には必ずそれらも送付される。Bまたは他の当事者がAのために複数の証明書を作成する場合もあると考えられる。例えば、ある証明書ではAが自分自身の身分証明を確実に行なうことを許可するがそれ以上の権限を指定することはしない。別の証明書では連帯署名を要求することなくある限度の金額をAに委任する。さらに別の証明書ではそれより多額を委任するが、1つ

またはそれ以上の連帯署名を要件とする。さらに別の証明書ではさらに異なる金額および／または権限上の制限および／または連帯署名条件に従って他の者に副証明を与えることを許可することができる。

Bが第5図に示すような証明書をAに対して作成したと仮定すると、Bが連帯署名者を要求しなければその証明書は完成したことになる。しかし、Bに対してAの証明書を作成する権限を与えた証明書がBに対して連帯署名者を要求している場合がある。1つまたはそれ以上の合同署名および／または副署名の要件が存在する場合もある。

第6図は当事者CがAの証明書を合同証明する時にとる段階を例示したものである。合同署名者を必要とする要件がB自身の証明書の中に特定されていたものとする。この場合、Bの証明書と共に署名されて伝送された対象物（この場合Aの新

証明書）は、Cの合同署名も該対象物上になければ受け手側によって拒否されることになる。

第6図に示すように、このような合同署名が必要な場合、Aに対するBの証明書のコピーが、該証明書に合同署名しなければならないC(132)に送付される(130)。そこでCは(132)Aの証明書を検証し、該証明書のパブリックキーがAに属するものであるかどうかを第3図に関連して説明した方法に従って確認する。

次にCは委託されている金銭的レベル、信用レベル等を含めて証明書の中に明示されている署名された権能および権限を検証する。Aに対するBの証明書の全ての欄が適正であると判断すると、Cは自分が署名を行なうのに用いる自分自身の証明書を選択する(126)。Cは彼自身の証明書138を用いてBのAに対する証明書132に署名する(130)。Cが自分の証明書に署名すると、彼の署

名は第6図の134と136に示すようにBの署名および他の副署名者と本質的に並記された状態となる。従ってCはAの証明書を承認する際にBと同じ位の注意を払う必要がある。Aの証明書が一旦作成されると、副署名者の誰も該証明書を変更することはできない。そうすることは、それより前の署名が成されなかったであろう本質的に異なる対象物を作り出すことになるためである。Cが証明書を承認しない場合は署名することを避けねばならず、また別の証明書を構成してそれに必要とされる全ての当事者に再び署名してもらうようにしなければならない。CがAに対するBの証明書にCの合同署名を付け加えると、Aの証明書パケットはAに対する証明書138と、Aの証明書に対するBの署名パケット134と、Aの証明書に対するCの署名パケット136から成る。

Cの署名パケットに関しては、Cが該証明書に

有効に署名するためにはAの証明書のどの面をCが承認しようとしていてもその面をカバーするに足る権限をCに与えるC自身の証明書を1つ選択しなければならない点が注目される。Cにこのような証明書が無ければ、将来の受け手が彼の証明書を十分な権限をもたないとして拒否するであろうから、証明書に有効な署名を行なうことは不可能になる。

Cの証明書も別の当事者による副署名を必要とする場合があることが注目される。その場合、Cは該証明書と全ての関連署名をCの署名に副署名する特定の当事者、例えばDに送付する。資料を受け取ったDは新証明書に関してCと同じ検証段階を踏む。承認の場合、Dは自分の署名を一連の署名に加える。但し、Dは元の証明書に対してではなく、Cの署名に署名するのである。すなわち、Dの署名の対象はCの署名の対象（この場合はA

に対する証明書）ではなく、Cの署名そのものを対象とするのである。従ってこの副署名は、対象物を同じくする別の署名にすぎない合同署名とは異なるものである。

合同署名および／または副署名は所要の程度まで重複することができる。すなわち、Dが合同署名を必要とする場合、このパッケージをDの合同署名者候補に送ってCの署名の承認を得なければならない。これは合同副署名となろう。同様に組織的な階層制の中では、Dが副署名を必要とする場合もあろうが、この場合は誰か他の人がDの署名に署名する必要が生じる。

以上に説明したように、一次対象物（購入注文書等）およびその関連署名を受け取った人は、受け取った資料を処理して、該対象物がパブリックキーの所有者によって署名された時点での資料と同じかどうか確認しなければならない。署名の検

証および対象物が改ざんされていないかどうかの検証を行なう方法については、第3図に関連して上で説明した通りである。

さらに、受け手は署名者の身元が正しいこと、また受け取った対象物に含まれる委任を行なうのに必要な権限を署名者が組織内で与えられているかどうかを検証する必要がある。対象物（例えば購入注文書）の送り手は、受け手が確認作業を行なうのに必要となる全世代の先行証明書および署名（組証明書を含めて超証明書まで）を送付する義務を有する。

対象物およびその署名を確認する際、受け手側は例えば次のような手続きをとることができる。まず受け手は一次対象物が少なくとも1つの署名を有していることを確認する。第7図に示した例では、一次対象物150が4つの関連合同署名152, 168, 180, 200を有しており、その各々に関連証明

書154, 170, 182, 202がそれぞれ付随している。

証明書154は証明書170, 182, 202の所有者による合同署名とこれらの特定証明書を用いた証明書162, 166の所有者による副署名を必要とするように作成されたものである。証明書154そのものは、署名156によって証明されるように証明書158の所有者によって認可されている。

この例では、証明書154の所有者が証明書162, 166の所有者による所要の副署名160, 164の他、所要の合同署名168, 180, 200も獲得している。

その署名168に関して確認を行なうためには、証明書170の所有者が彼の証明書に対する委任を含んでいなければならない。彼の証明書は証明書174の保有者によって署名されているが（172によって証明されるように）、174の証明書は174の署名172を完全に有効と認めるためには176の所有者による合同署名が必要であることを条件と

して挙げている。過去の何れかの時期に成された署名176は174の合同署名要件を全て満たしており、それによって170の使用が認可（批准）されたことになる。

182の所有者による合同署名180を見ると、特定証明書186を用いた186の保有者による副署名が証明書182に必要であることが分かる。証明書182の保有者は実際に188の保有者による副署名を獲得している。ところが、証明書186は186そのものによる署名は何れも証明書190,194の保有者による（それぞれの証明書を用いた）副署名を行なうことを要求している。証明書190,194の保有者は188と192に証明されるように実際に184に副署名を行なっている。もう1つ上のレベルにおいては、証明書194が194による何れの署名にも、署名196が獲得された証明書198の保有者による副署名を付すことを要求している。証明書

202は副署名を必要としない。

全ての証明書は、それ自身が先行証明書によって認可されている署名を伴わねばならない。全ての権限を辿って行くと、最終的には超証明書（または少数の超証明書の場合もある）の保有者によって署名された1組の証明書に行く着く。超証明書は「全世界の」全ての当事者に良く知られており、普及しているものである。

受け手側は供給される全ての署名を検証し、第3図に詳細に示した手順により各署名が目的とする対象物（対象物が一次対象物であるか、証明書であるか、別の署名であるかに関わらず）に正確に成されているかどうかを確認する。受け手は各署名がそれに対応して確認された証明書を含んでいるかどうかも確認する。

証明書が合同署名を要する場合、受け手はこれら所要署名（同一対象物に対する）が必要数ある

かどうかを確認する。証明書が副署名を要する場合は、指定された副署名から必要数の署名があるかどうかを確認する（副署名の対象物は署名である）。

次に全ての証明書を検査する。点検は特別の超証明書に関して行なうが、この超証明書は世界的に知られた信用のあるものであり、そのコピーが既に受け手側コンピュータに記憶されている。受け取った証明書が超証明書であると主張しているにもかかわらず受け手側が既に知っており容認しているものと等しくない場合、拒絶が生じる。超証明書が然るべく認知された場合は、有効性確認プロセスが続行される。

さらに、超証明書を除く全ての証明書が少なくとも1つの署名を有していることを確認する点検を行なう。上述のように、提示された全ての対象物に対して必要な全ての連帯署名が存在するかど

うかを確認する点検も行なう。さらに、先行証明書が副証明書の署名者に対して該証明書に有効に署名し得るだけの権限を付与しているかどうかを判断する点検を行なう。

この時、証明書の信用値は先行証明書（すなわちその署名者の証明書）と一致していなければならない。一例を挙げると、下記の信用欄の組合せが有効である（先に特定した例を用いて）。

現在の信用値	信用値および先行（保証人の）証明書
0	1
0	2
0	3
1	2
1	3
2	2
2	3

さらに、証明書に金銭的条件が明示されていれば、それにも注意しなければならない。ある証明書によって許可される限度はその先行証明書の限度を超えてはならない。また、各証明書の失効日がその先行証明書の失効日と矛盾していないか確認する点検も行なう必要がある。一例を挙げると、各証明書に示された失効日が該証明書に依拠する各署名の日付を超えていることを確認する点検を行なうことができる。場合によっては、既に失効した証明書によって管理されている資料を拒否するのが望ましいこともある。

授権の輪が「閉じられている」（授権の輪の最後の人が最初の人に権限を与えることによって一連の証明書を虚偽に作成する）ことを検出するためには、全ての権利が最終的に権威ある超証明書から出ていることを確認することが必要である。こうすることで相互に証明し合う虚偽の、または

作為的な証明書の連鎖がうっかり許可されて、確認プロセスをすり抜けてしまうことがなくなる。

これを達成する1つの方法として、超証明書を用いて頂上からスタートする一連の繰返し動作で証明書に照合の示しを付けて行く方法がある。繰返し毎に証明書の走査を行ない、そのプロセスで照合の示しの付いた先行証明書を少なくとも1つ有する証明書を次に検証する。既に十分に「照合済みの」先行証明書（有効な合同署名および副署名の要件に関する考慮も含めて）によって必要な全ての権限が委譲されていれば、この証明書も照合済みとみなされる。照合されていない証明書があれば、これらは供給されてはならなかった「孤児」であり、無視される。

署名および証明書が有効確認されると、（超証明書の究極的権限に基いて）、最後の段階として一次対象物に固有の委任行為がその当面の（照合

された）（合同）署名者に与えられた権限の範囲内であるかどうかを確認する。これはその署名者の証明書を用いて一次対象物に帰属する価値を考慮することによって行なわれる。

超証明書の使用により全ての権限が究極的には権威のある源から出たものであることが保証され、保護が与えられるが、本発明は必ずしも1人の超証明者を含む証明方法に限定されるものではない。本発明では、複数の超証明者の使用を可能にすることも含まれる。これらは、おそらくは全く異なる権限付与階層（例えば政府部門対私的部門）の頂点を反映する全く独立した源によって管理される証明書となるはずである。

各使用者は、ある時点で何らかの方法でコンピュータシステムに認識信号を送ることによって各超証明書を「受理」し、使用者の信用を認識させる必要があることに注意されたい。これを行なう

1つの方法として、使用者が各超証明書の暗号化コピーまたは署名コピー（またはそのハッシュ）を保持する方法がある。

複数の超証明者を使用すると、1つのグループに全部の超証明責任が集中するのを防止することも可能になる。例えば、虚偽の証明書を作成することによって理論的には誰かのために偽造品を作成し得る実体が1つだけ存在することが分かれば不愉快であろう。異なる権威ある超証明者の間に超証明権限を配分すれば、このような心配も軽減することができる。この場合、各超証明者が完全に独立して働くが、各証明書が合同証明者として他の超証明者を特定的に必要とすることになる。これによって1つの組織内で孤立して生じた腐敗がシステム全体に及ぶ可能性を実質的に無くすことができよう。例えば、証明を受けようとする組織は、彼ら自身の高レベルの主証明書に別個の実

体からの確証を得る必要が生じる。大組織の場合も同様に、組織内部での孤立した腐敗の危険に対する多重保護措置を設けるためには、彼ら自身の主証明書を合同署名を必要とするように構成すれば良い。

第8図はある当事者から別の当事者へディジタル文書として電子伝送される覚書の一例を示したものである。文書を伝送する側の当事者は通信文のメッセージ部分（"Digital Signature"部分より上に示される）を生成した後に、第1図に示したキーボード／ブラウン管1の制御キーを押してディジタル署名と該ディジタル署名を管理する証明書の要約を構成する（その例を第8図に示す）。

第8図に示したディジタル署名は第2図に関連して上述したように作成することができる。長々と連なる16進データから成る署名およびシールは、

ことができる。この他要約データには第5図のブロック116で挙げたデータの何れかまたは全部を含ませることができる。

ディジタル署名および証明書が受け手側のコンピュータファイルに着信すると、第3図および第7図に関連して上で詳述した手順に従ってその有効性確認が行なわれる。この時、第8図に示した文字は上記手順で該署名が有効であり、然るべき許可を受け認証されていると判断されるまでは印字されないことが注目される。

本発明によって提供されるこの他のディジタル署名の改良点として、印字の対象となる対象物について「ホワイトスペースハッシュ」が計算される点がある。後述するようにこのホワイトスペースハッシュは署名の一部となり、対象物、対象物のハッシュ、対象物の種類および任意の注記と共にハッシュされ、ディジタル署名の一部となる。

第9図に関連して後述するように対象物のハッシュ、対象物の種類、署名日、シール等のデータを含んでいる。

さらに、第8図は第2図のブロック38に示したようにディジタル署名を作成するのに使用した証明書を同定するディジタル署名を支配する証明書の要約を含んでいる。証明書情報の要約には該証明書を32の16進数で独自に同定する証明書I.D.のような証明書から抽出されたデータが含まれる。証明書I.D.の32の16進数は証明書に含まれるデータのハッシュであり、従って該証明書を独自に表すものである。よって2つの証明書が同じI.D.をもつことはない。

また、要約データの中には証明の日付の他、例えば証明される側が取扱う権限を与えられた認可金額の限度等も含む。必要に応じて機密レベルと信用レベルのデータも要約データの中に含ませる

これが最終的に署名者のプライベートキーで処理されてシールが作成される。

ディジタル伝達される文書の多くが最終的には第8図に示した覚書のように印字される。このような文書がコンピュータ生成されてディジタル署名されたものであれば、例えその文書がコンピュータメモリにもはや記憶されていなくても、将来において署名および文書の有効性確認を可能にするために必要になることがある。

印字されたディジタル署名の検証にはいくつかの問題がある。単に文書をコンピュータに再入力して確認署名ハッシュの「指紋」を再計算するだけでは多くの理由によって役に立たないと考えられる。例えば、元のコンピュータ文書はおそらくタブ、空白、改行制御文字その他の印字不可能な制御文字を含んでいたものと思われるが、これらは印字出力からだけでは確認することができない。

ディジタル署名は元のコンピュータファイルの正確なビット対ビット画像に基くものであるため、ほとんどの場合文書を当初生成された通りにビット対ビットでリタイプすることは本質的に不可能である。例え使用者が元と同じに見えるプリントアウトを得ることができたとしても、元はタブ、スペースその他の制御文字の混ざり方が多少違っていたであろうと考えらえる。

本発明は、署名がコンピュータによる検証用と同時に、文書を用紙に印字した状態から再入力して再確認する必要が生じた場合の緊急再検証用としても生成される文書のディジタル署名法を採用することによってこの問題を解消する。本発明によると文書形式のコンピュータメッセージ用のディジタル署名は2つの別個のタイプのハッシュ値を含む。第1のハッシュ値はファイルの厳密なビット対ビットデータに関するものであり、上述の

ようなディジタル署名を構成するのに使用される。これによってコンピュータが読取れる形で入手し得る限り正確の原文書の確認を行なうことができる。

さらに、第2の補助的ハッシュ値がファイル内の同じデータに関して取られるが、第2ハッシュ値に使用されるデータは下記の方法で「ホワイトスペース正規化」される。このホワイトスペース正規化によってある将来の時点でデータをプリントアウトから再入力することが可能になり、しかも原文書にどのような種類の印字不能、知覚不能な制御文字が存在したかについて考慮する必要がない。ディジタル署名の中にホワイトスペース正規化したハッシュ値を含ませることによって、原文書の印字版を後日真正として検証することができる。

この時、ホワイトスペースハッシュ値の計算が

回復した文書に関して行なわれ、この計数値がディジタル署名およびシールのデータと比較される。記憶されているホワイトスペースハッシュ値と計算値が一致すれば、該文書は真正として検証される。

文書を「正規化」する方法は多数あるが、下記のアルゴリズムがその一例である。

ホワイトスペースハッシュの計算方法について説明する前に、第8図に示された書状およびその他同様に生成された文書は一般にアスキー(ASCII)ファイルとして記憶されることが特記される。このアスキーファイルは改行制御文字、タブその他の制御文字を含む。このようなコンピュータファイルから生成されたハッシュ値がコンピュータファイル内の各ビットの関数となる。従って例えば制御文字を1つでも変更すれば異なるハッシュ値が生成されることになる。

第9A図および第9B図に関連して以下に説明するホワイトスペースハッシュ機能により、ディジタル文書を受け取った人はそれが印刷文書そのものにすぎないのかあるいは伝送されたコンピュータファイルであるのかディジタル文書の真偽を検証することができる。第9A図を参照すると、まずホワイトスペースハッシュを生成しようとする文書を入力することによってホワイトスペースハッシュが計算される(250)。ホワイトスペースハッシュ処理ルーチンが始動されて、新資料のハッシュを生成する(252)。この時、ホワイトスペースハッシュの生成に関連する全てのレジスタがクリアされる。

その後、入力し終った文書を印字状態と同じ様に行毎に分割する。この作業は通常の場合改行文字および/または行送り文字を調べることで行なわれる。文書を行毎に分割した後、文書の第1行

（または次の行）を検索する(254)。

第1行の検索後、ループを入力してその行の処理を行ない、最初の点検でファイルの終わりまで到達したかどうかを判断する。ブロック256での点検結果でファイルの終わりに到達していれば、ハッシング関数処理ルーチンから最終ハッシュ値を検索する(258)。次にこの最終ハッシュ値を後述するようにディジタル署名の一部として用いる(260)。

ブロック256での点検でファイルの終わりに達していないことが分かれば、検索した行をメモリのワークエリアに移す(262)。メモリのワークエリアでは、全てのタブ文字をスペース文字またはブランク文字に変える(264)。その後、その他印字可能な文字にならない全ての制御情報を削除する(266)。この時残った制御情報でフォント、スタイル、下線、イタリック体等の設定に使用され

る情報は全て除去する。1つまたはそれ以上のブランク文字を生じる制御情報はスペースに置き換える(268)。従って1行の中に出て来る複数のブランクが1つのブランクに置き換えられる。このようにして、文書が一般にはアスキー（ASCII）の基本文字にまで縮小される。

その後、行の初めの部分と終わりの部分を点検し、導入ブランク、後続ブランクを全て削除する(270)。次に1行全部がブランクかどうかを判断する点検を行なう(272)。もしそうであれば、全部がブランクである行を削除し、ルーチンを分岐してブロック254に戻り、文書の次の行を検索する。

またその行全部がブランクでない場合は、第9B図に示すように、複数個連続して続くブランクがあればそれを1つのブランクに変更する(274)。さらに、プリンタの中には大文字しか印字しない

ものもあるため、残った全部の文字を大文字に変更する(276)。この段階は上述のようにプリンタの中には大文字しか印字しないものがあることから処理方法を標準化するために行なうものである。受け手側のプリンタが全て大文字と小文字を混合して印字できるものであれば、この段階を省略することも可能である。

その後、区切り文字を用いて行の終わりを独自にかつ明確に同定することにより行と行と区別しておくようにする(278)。例えば、新行文字のような特殊文字を再挿入すれば、その時正規化された行を分離することもできる。この時使用する制御文字は文書本文の中に登場することのない文字にしなければならない。あるいはまた、行の頭にプレフィックスを用いて改訂行の長さを同定することもできる。上述のような処理をした改訂行をデータとしてハッシング関数処理ルーチン(280)

に送り、それによって上述のような本文の行を明確に同定するハッシュ値が決定される。

その後、ブロック254において文書の次の行を、ブロック256においてファイルの終わりに最終的に到達したと判断されるまで検索して行く。文書全体の処理が終わった時結果的に得られたハッシュ値が該文書のホワイトスペース正規化ハッシュ値であり、これを後述するようにディジタル署名の一部として用いる。

第10図は計算により得たホワイトスペースハッシュをディジタル署名に用いる方法の一例を示したものである。また第10図は本発明により複数の文書および／またはファイルに集団的に署名する方法の例も示している。

第10図に示す「多重文書」は添え状300、書状302(関連署名および証明書303を有する)、スプレッドシート304およびグラフィックファイル

306 等の関連するがそれぞれ別個の対象物を複数個含んでいる。書状302 は例えば添え状100 に名を挙げた受け手に送付される書簡とすることができる。

このディジタルパッケージにディジタル署名308 を署名する。またパッケージは上述のようにディジタル署名と関連するシール310 を含む。ディジタルパッケージの中には証明書と先行証明書312 も含まれており、これによって受け手は上に詳述したように署名が有効であり然るべき権限を与えられていることを納得のいくまで立証することができる。

第10図の308Aに示したデータ構造はディジタルパッケージと共に伝達される署名の定義308 を拡大したものである。このデータ構造308Aをハッシング320 にかける。次にハッシング機能320 からの出力を署名者のプライベートキーを用いて処理

の関係も明らかにすることができる。

第10図に戻ると、上述のように署名の定義308 の拡大が308Aに示されている。第2図に関連して既に説明したように、署名の定義にはディジタルパッケージに署名した日時に関するデータの他、該パッケージに関する解説全般が含まれる。また、署名の定義には上述のように委任証明書のI.D.を含む署名者の証明書および/または関連パブリックキーが含まれる。

その後、署名される対象物のリストが上述のディジタルパッケージの4つの部分（すなわち添え状、書状、スプレッドシート、グラフィックファイル）の各部に選別しながら組入れられる。リストの各対象物と関連するのが対象物の種類に関する定義であり、これによって例えば該対象物が購入注文書か、別の署名または証明書か、書簡かが表示される。

する(322) 。ブロック322 の出力は310Aに示すようにディジタル署名のシールであり、310 において伝達されるディジタルパッケージに組込まれる。

第8図に示したように、署名およびシールを表すデータは伝達されるディジタルパッケージの下部に16進表記法または8進表記法で印字される。この情報に検査合計その他のエラー検出用および/または修正用コードを含ませて、打ち間違いのデータがあればそれを容易に検出できるようにするのが望ましい。上述のようにディジタル署名をパッケージのディジタルプリントアウトの一部として含ませることによって、印字した文書を後述するようにホワイトスペースハッシュ値を用いて再検証することが可能になる。

また集合署名リストがあれば、例え全ての文書を入手できなくても任意の特定文書を署名されたものとして検証することができ、その他の文書と

署名される文書のリストについて説明すると、第1文書（例えば添え状）から開始して各文書のハッシュ313A, 315A, 311, 319 をちょうどそれが伝達されようとしている時の状態で計算する。さらに添え状と書状のホワイトスペースハッシュ313B, 315Bを、第9A図および第9B図に関連して上に詳しく説明したように計算する。また、書状と関連する署名および証明書303 からハッシュ316 を取出す。スプレッドシート304 とグラフィックファイル 306 は2進ファイルであるため、これらのファイルについてはホワイトスペースハッシュを計算しないことが注目される。

上に挙げたハッシング関数を用いてシール310Aを作成すると、結果的に得られたシールは署名の定義308Aに出て来るデータによって作成されたものに間違いない。従って受け手側はシールから通ることによって署名の定義に含まれるデータの真

偽を検証することができる。

上述のように、ホワイトスペースハッシュを計算して記憶させる目的は、将来において唯一のコピーが受け手のハードコピーファイルにある印刷版であるディジタル文書の検証または認証が必要になる場合があることにある。第11図の流れ図に従ってこのような文書の再検証を行なうことができる。

第11図に示した印字文書335は例えば第8図の文書とすることができる。ブロック327に示すように再検討サブルーチンから使用者に対して文書の主要部を再入力し、それを印字文書にある通りにタイプするように指示がある。この時、ホワイトスペース正規化によって全ての多重ブランクを無視しているため、文書のブランクの処理を繰返すように入力する必要はない。

文書主要部の入力後、ホワイトスペースハッシ

ュを第9A図および第9B図に関連して上で説明したように計算する(329)。第11図に示したホワイトスペースハッシュ値は数値Dとして記憶される(330)。

その後、再検証ルーチンから使用者に対し、署名およびシールをその通りに再入力するように指示がある(331)。署名およびシールをその通りに入力しなければならないため、16進コードが正確に入力されたかどうかを判断する点検合計その他のエラー検出／修正コードを使用するのが望ましい。

再入力した署名およびシールは第10図の308Aと310Aに示した署名の定義およびシールのディジタル版（第11図ではそれぞれ333と335として表わされる）であることが注目される。331で入力されたコードは本来署名部分333がどこで終わりシール部分335がどこで始まるかを定義するコード

である。

ブロック339に示すように、333に示した署名部分のハッシュを求め、ハッシュ値Aを記憶する(340)。

その後、署名のシール(335)を署名者のパブリックキーで処理して(337)後の点検に用いる16進値Bを生成する(338)。数値Aで示される署名のハッシュと数値Bとが等しければそのシールと署名は正しいものとして検証される。従って342での点検によって示されるように、AとBが等しければ当該文書が指定された証明書と共に署名されたとの判断が成される(344)。あるいはまたAとBが等しくなければ、当該文書は指定された証明書と共に署名されなかったことになる(345)。

ブロック337で使用されるパブリックキーは署名者の証明書を確認する署名情報333から獲得される。証明書のI.D.を用いて関連証明書の検索を

行なう(341)。この関連証明書はまだ有効で、受け手側のデータベースに残っているかもしれない。あるいはまた、既に文書保存されており回復を必要としたり、紙の上に記録されておりブロック341の方法で再入力を必要とする場合もある。

次にブロック343に示されるように関連証明書に示されている証明書I.D.がディジタル署名を管理する証明書の要約の下で例えば第8図に同定した証明書I.D.と符合するかどうかの点検を行なうことができる。符合する場合、その関連証明書は元の文書の受領時にシステムによって鑑定済みとして検証された真正の証明書であると推定される。別の方法として、その全ての先行証明書を捜し出して点検する方法により証明書を独立して検証することもできる。次にブロック337において証明書と関連するパブリックキーを用いて数値Bを生成する。

その後、333 で署名と関連付けられ、数値Cを有するホワイトスペースハッシュを334 に示すように記憶させる。次に数値CとDとを比較して当該文書が実際に署名された対象物であることを確認する。すなわち346 に示すように、CがDと等しければ当該署名が文書325 と対応すると判断される。CがDと等しくない場合、その署名は文書と対応せず(350) 、プロセスは中断される。署名が文書348 に対応し、しかもその署名が指定証明書344 により行われている場合、当該文書は特定の証明書351 の所有者によって署名されたものとして検証される。

第12図は受け手が多重文書／ファイルアーキテクチャを有する文書パッケージを受け取った時の署名検証方法を示したものである。受け取ったディジタル署名とシールを点検して、第10図に関連して先に説明した添え状300 と書状302 とスプレ

ッドシート304 とグラフィックファイル306 と署名定義欄308 と署名用シール欄310 とを含む文書ファイルにそれらが厳密に対応していることを確認する。このようにして、受け取ったデータが途中で損傷や損失を受けていないか、また文書が偽造または改ざんされていないかを判断することができる。

このような方法の主な利点として次の2点がある。

・個々の対象物を別個の実体として認識して別々に検証することができる。

・集合の中での各対象物の立場をパッケージの一部としての対象物の順位も含めて認識できる。

まず、各対象物300, 302, 304, 306 のハッシュをそれぞれ400, 402, 404, 406 に示したように計算する。次にハッシュ値B, D, F, Hを401, 403, 405, 407 に示したようにそれぞれ記憶させる。そ

の後、第12図において308Aに拡大して示した署名の定義を点検し、署名項目A, C, E, Gにアクセスする。項目A, C, E, Gはそれぞれ添え状のハッシュ、書状のハッシュ、スプレッドシートのハッシュ、グラフィックファイルのハッシュを表すものである。

署名が実際に第1対象物、すなわち添え状を反映しているかどうかを判断するために、項目Aとして示される署名における添え状のハッシュと添え状の計算ハッシュである項目Bとを比較する。AとBが等しければ、添え状のハッシュが署名の中に含まれている。数値CとD、EとF、GとHについても同様の比較を行ない、残りの対象物の各々が正しく署名の中に包含されているかどうかを判断する。各比較が符合していれば、300, 302, 304 および306 の主要部分が署名308 によって正確に反映されているとして検証される。

その後、署名の点検を行なってそれが正しいかどうかを確認する。410 に示すように、署名のハッシュを計算する。次に計算値Jを記憶させる(412) 。その後署名のシール310 を署名者のパブリックキーで処理して数値Kを得、これを記憶させる(416) 。

署名者のパブリックキーから抽出したハッシュである数値Kを点検して、それが再計算したハッシュJと符合するかどうかを判定する。次に418 に示すようにJとKが等しいかどうかを判定する点検を行なう。JとKが等しければ、実際に指定のパブリックキーを用いてディジタルパッケージ内の各対象物に示された順序で注記をつけながら署名したものである(420) 。従ってこの署名はパッケージに対する有効ディジタル署名を表すものである。次に署名と証明書の点検を行なって、第7図に関連して説明したようにそれらが実際に権

限を与えられていることを確認する。

以上、現時点で実際的な実施態様と考えられるケースに関連して本発明の説明を行なって来たが、本発明は開示された実施態様に限定されるものではなく、請求項に記載の範囲とその精神に該当する各種の変更や等価の構成も包含するものであると理解されるべきである。

4．図面の簡単な説明

第1図は本発明の例示的実施態様による暗号通信システムを示す構成図、第2図は本発明の例示的実施態様によるディジタル署名の作成方法を示す流れ図、第3図は第2図に従って作成したディジタル署名の検証方法を示す流れ図、第4図はディジタル署名に対する副署名の作成方法を示す流れ図、第5図は本発明の例示的実施態様によるディジタル証明書の作成方法を示す流れ図、第6図は証明書に合同署名を加える方法を示す流れ図、第7図は伝達されたメッセージの受け手が署名および証明書を検証する方法を示す流れ図、第8図はディジタル署名部を含む電子送信覚書の一例、第9図A-Aおよび第9図B-Bはホワイトスペースハッシュ関数の計算を伴う処理方法を示す流れ図、第10図は本発明による多重文書パッケージの署名方法を示す図、第11図はホワイトスペースハッシュ機能を用いて印字文書の再検証を行なう方法を示す図、第12図は多重文書／ファイルパッケージに関する署名検証方法を示す図である。

出願人 アデイスン・フイッシャー
代理人 弁理士 川口義雄
代理人 弁理士 中村至
代理人 弁理士 船山武

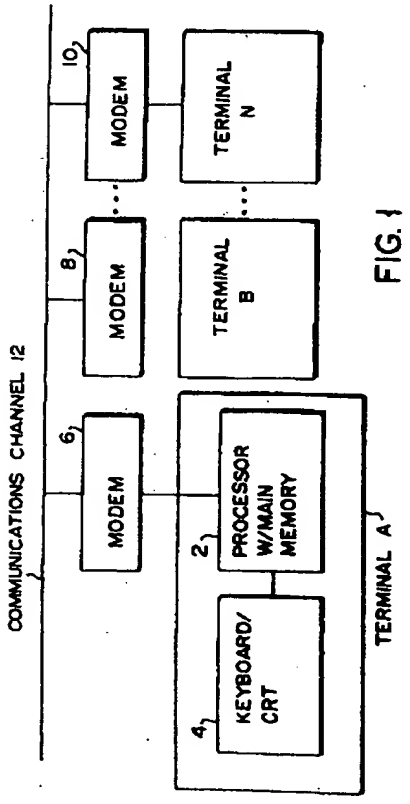


FIG. 1

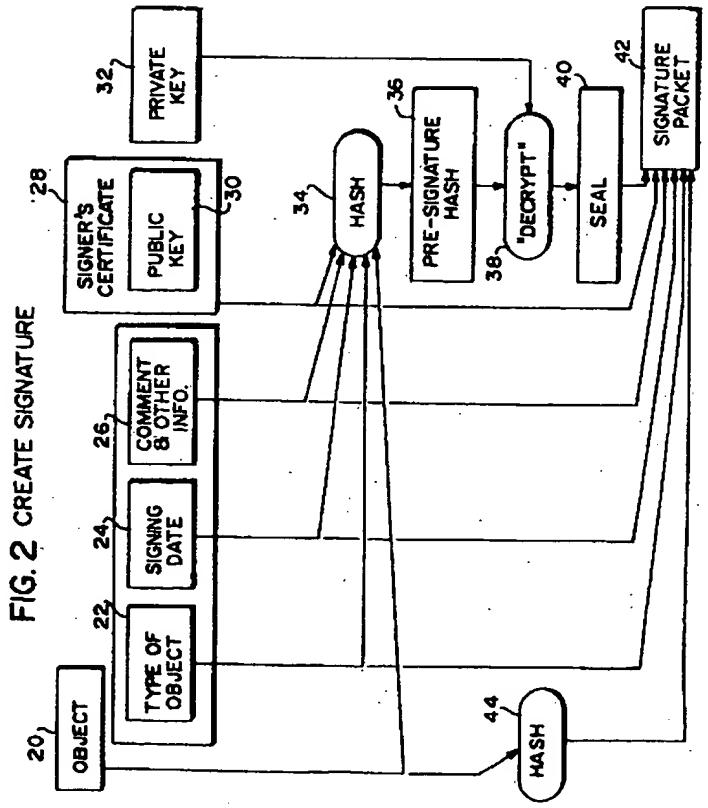


FIG. 2 CREATE SIGNATURE

FIG. 3 VERIFY SIGNATURE

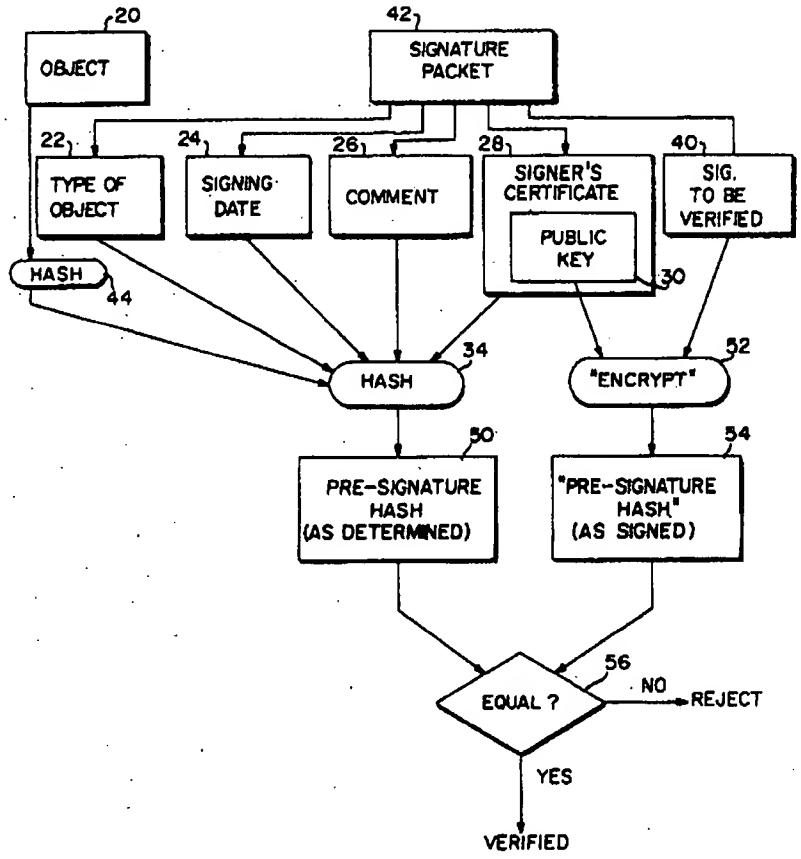


FIG. 4 "C" CREATES COUNTER-SIGNATURE FOR A'S SIGNATURE

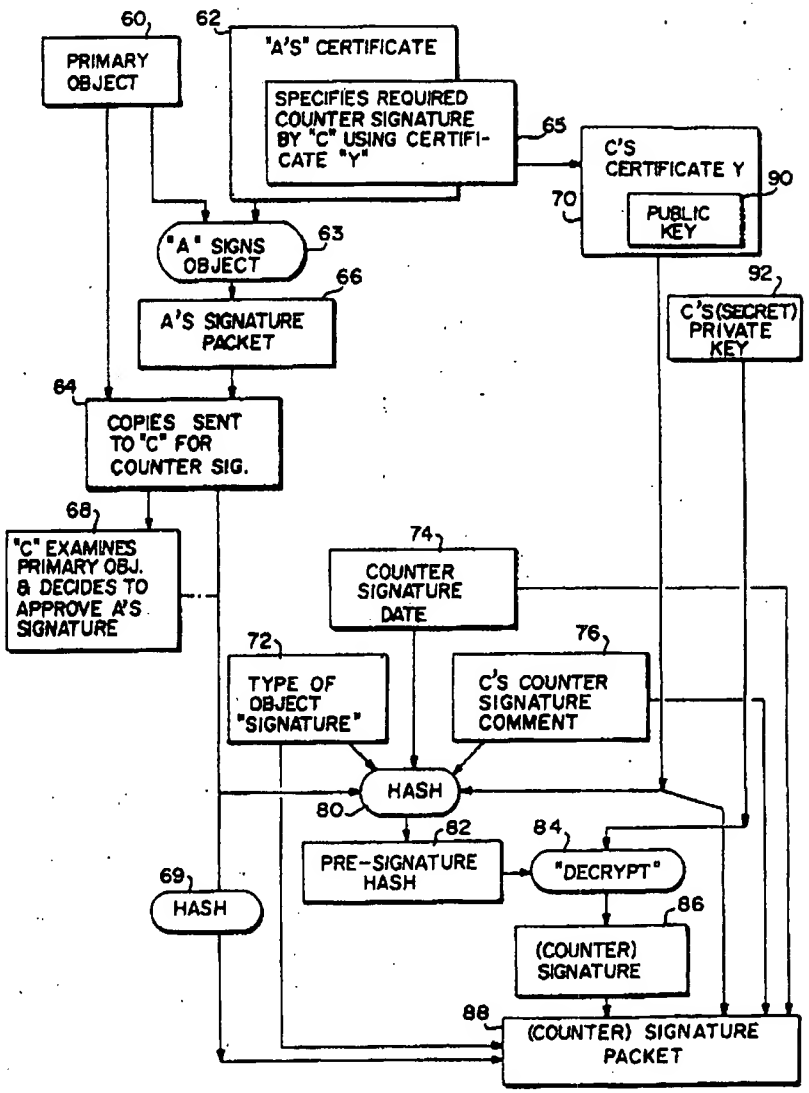
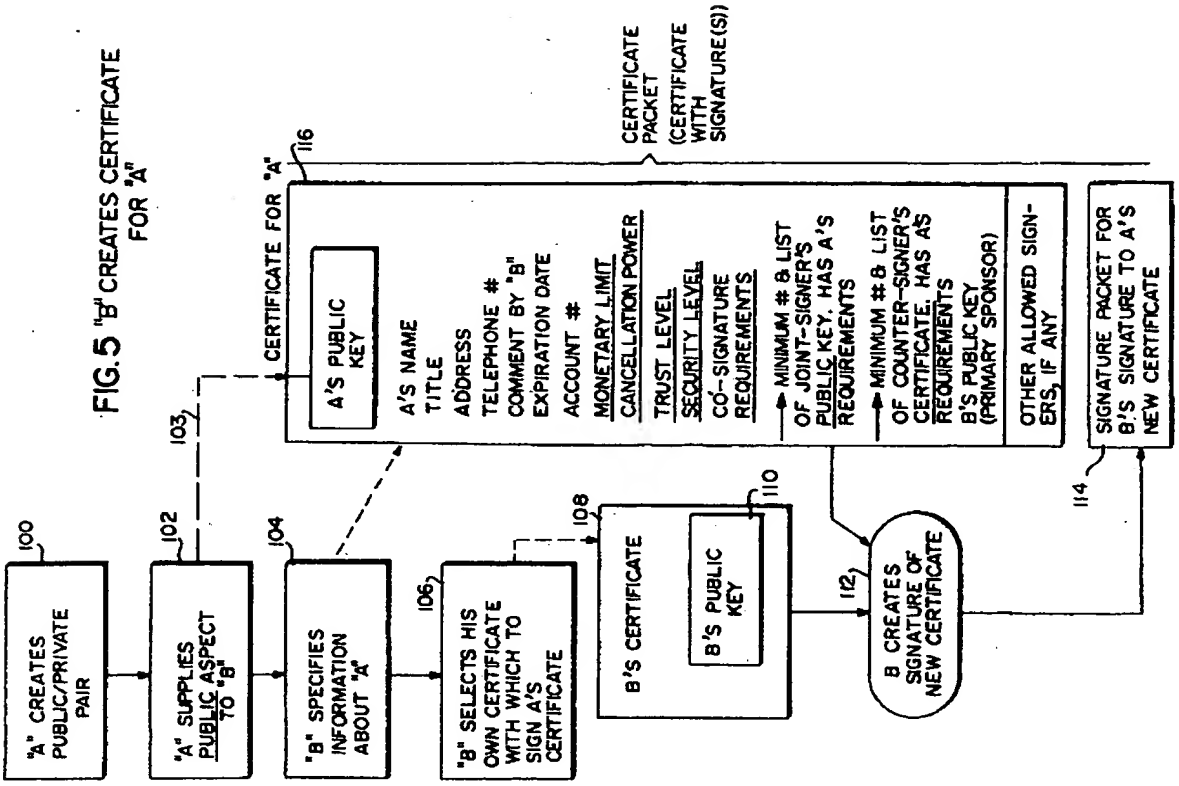


FIG. 5 "B" CREATES CERTIFICATE FOR "A"



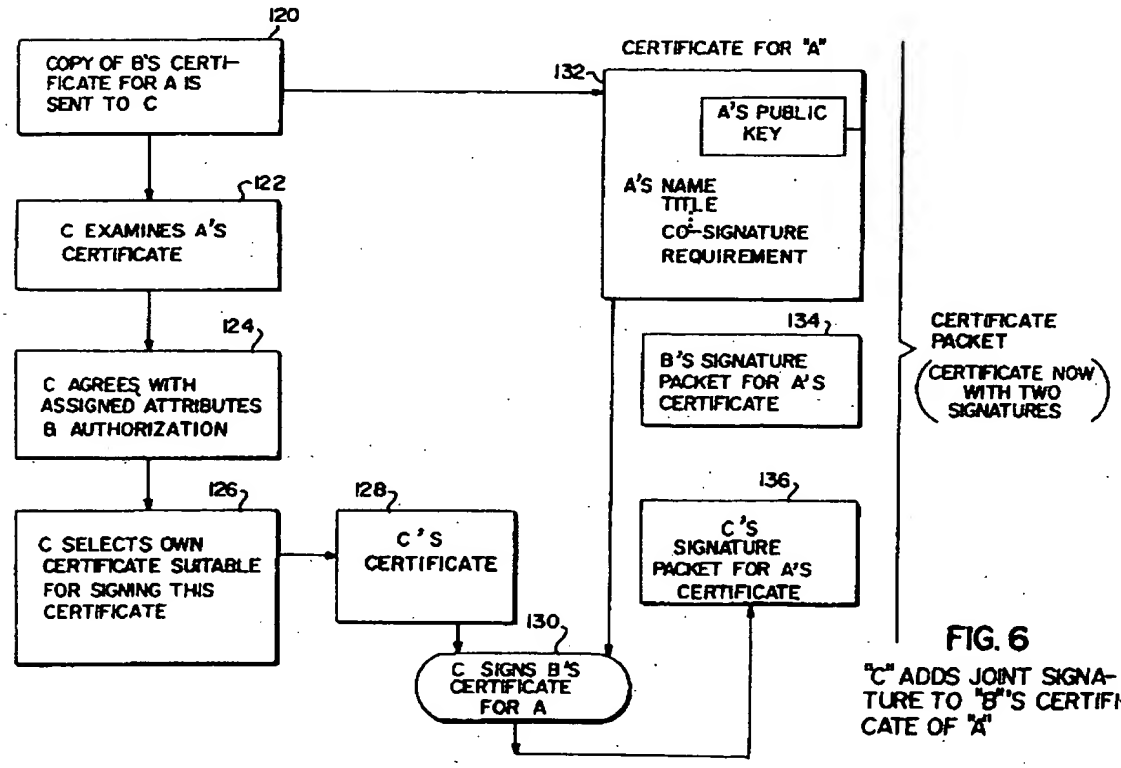
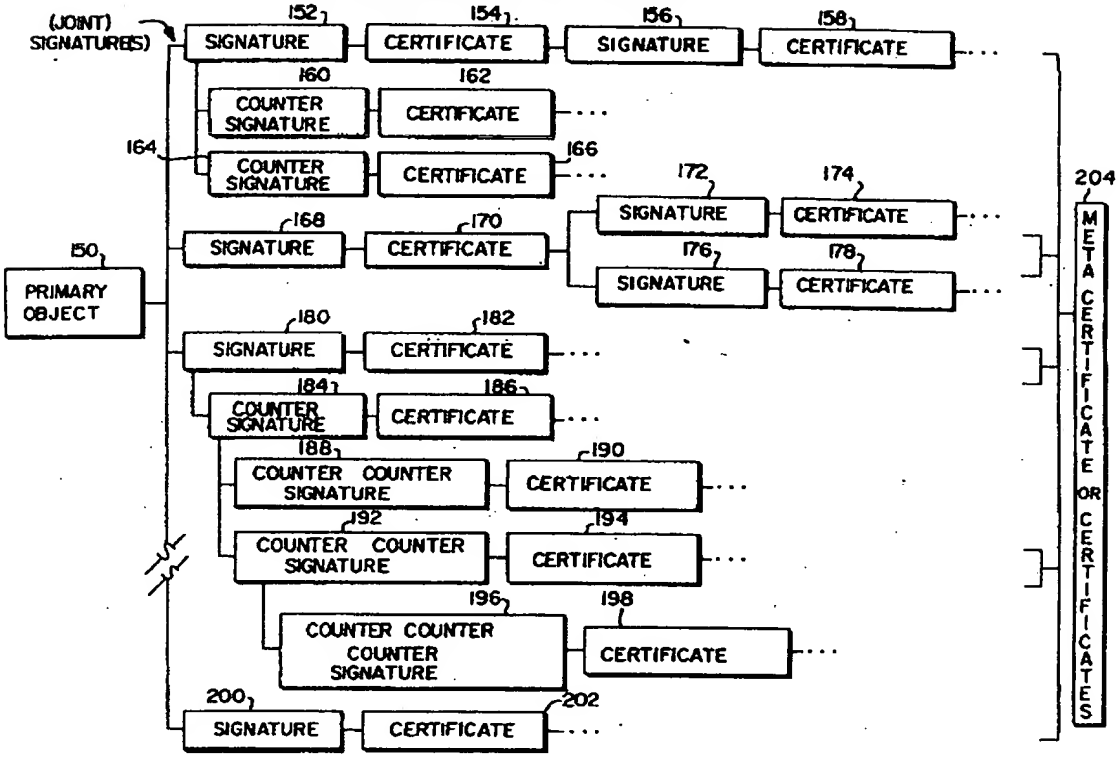


FIG. 6

"C" ADDS JOINT SIGNATURE TO "B"'S CERTIFICATE OF "A"

FIG. 7 VALIDATION STRUCTURE (EXAMPLE)



To: John Haberford, Universal Widgett Corporation
From: Bob Blakely, Hattersfield Marine Builders
Date: 14 July 1988, 10:26 am EDT
Subj: Widgets received

Dear John,
We received the July 12 Shipment of widgets, and found only one item of damage, namely a nick in the paint of widget number #4688219-A3367.

Thanks.

Digital Signature:
Signature Date: 14 Jul 1988, 10:34 am EDT
Signature & Seal:
65263317 9E035673 CAA32E6F B21988C8 0ED113F6 571B060B B1B88EEE DCE1F1B7
4DB488A8 801CE95B 30F289EC EADBFD96 C831772D 5895D945 E2E7E5AC CD510CFC
C8CF370C 2F87AB01 5638DD0F 3FBA3D7C A1583BF1 147C4477 060D28F7 3921F90E
F8EA6F90 75DA4EDF FACCBE05 A62D41E1 6B34789E 35CE84CF 0ED7DF91 35713371

Summary of Certificate governing digital signature:
Certif ID: FB8FD88F B9EDC829 82D8C468 37619831
Certif Date: 01/23/88 04:00 pm EST
Authorized Money Limit: 5000 $US
Id of certified:
Robert J. Blakely
Production General Manager
Hattersfield Marine Builders
Naples, Florida 33942

Printing notes:
Page numbers added by print function, not part of document.

FIG. 8

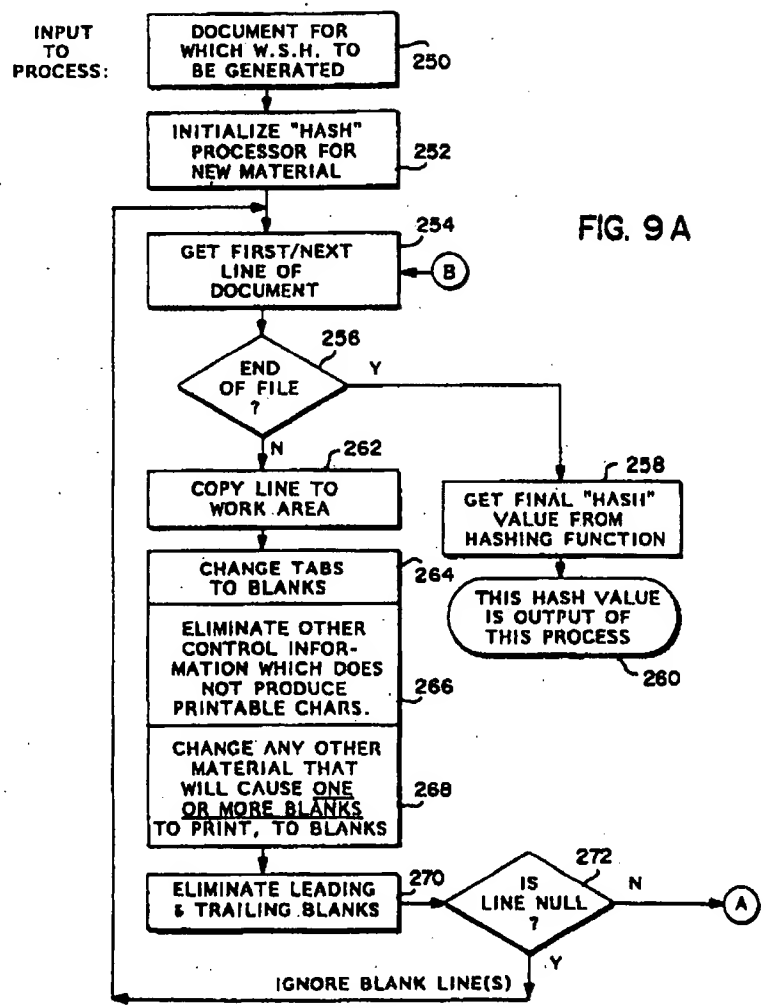
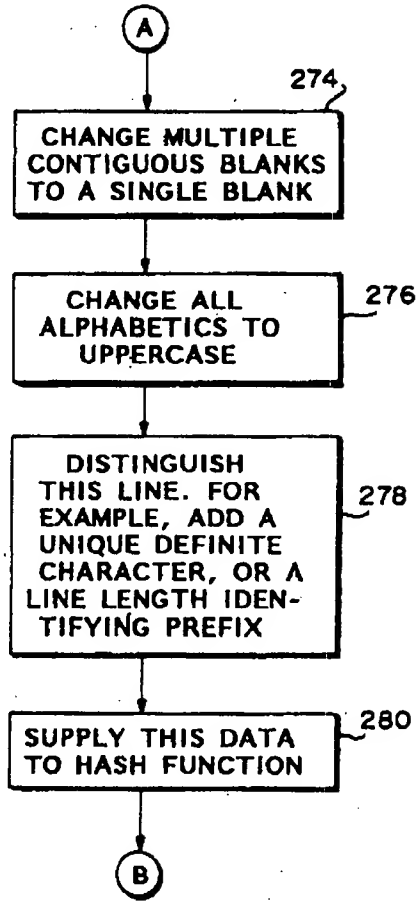

INPUT TO PROCESS:
DOCUMENT FOR WHICH W.S.H. TO BE GENERATED
250
INITIALIZE "HASH" PROCESSOR FOR NEW MATERIAL
252
GET FIRST/NEXT LINE OF DOCUMENT
254
B
END OF FILE ?
256
Y
N
COPY LINE TO WORK AREA
262
GET FINAL "HASH" VALUE FROM HASHING FUNCTION
258
THIS HASH VALUE IS OUTPUT OF THIS PROCESS
260
CHANGE TABS TO BLANKS
264
ELIMINATE OTHER CONTROL INFORMATION WHICH DOES NOT PRODUCE PRINTABLE CHARS.
266
CHANGE ANY OTHER MATERIAL THAT WILL CAUSE ONE OR MORE BLANKS TO PRINT, TO BLANKS
268
ELIMINATE LEADING & TRAILING BLANKS
270
IS LINE NULL ?
272
N
A
Y
IGNORE BLANK LINE(S)

FIG. 9A

FIG. 9B


A
274
CHANGE MULTIPLE CONTIGUOUS BLANKS TO A SINGLE BLANK
CHANGE ALL ALPHABETICS TO UPPERCASE
276
DISTINGUISH THIS LINE. FOR EXAMPLE, ADD A UNIQUE DEFINITE CHARACTER, OR A LINE LENGTH IDENTIFYING PREFIX
278
SUPPLY THIS DATA TO HASH FUNCTION
280
B

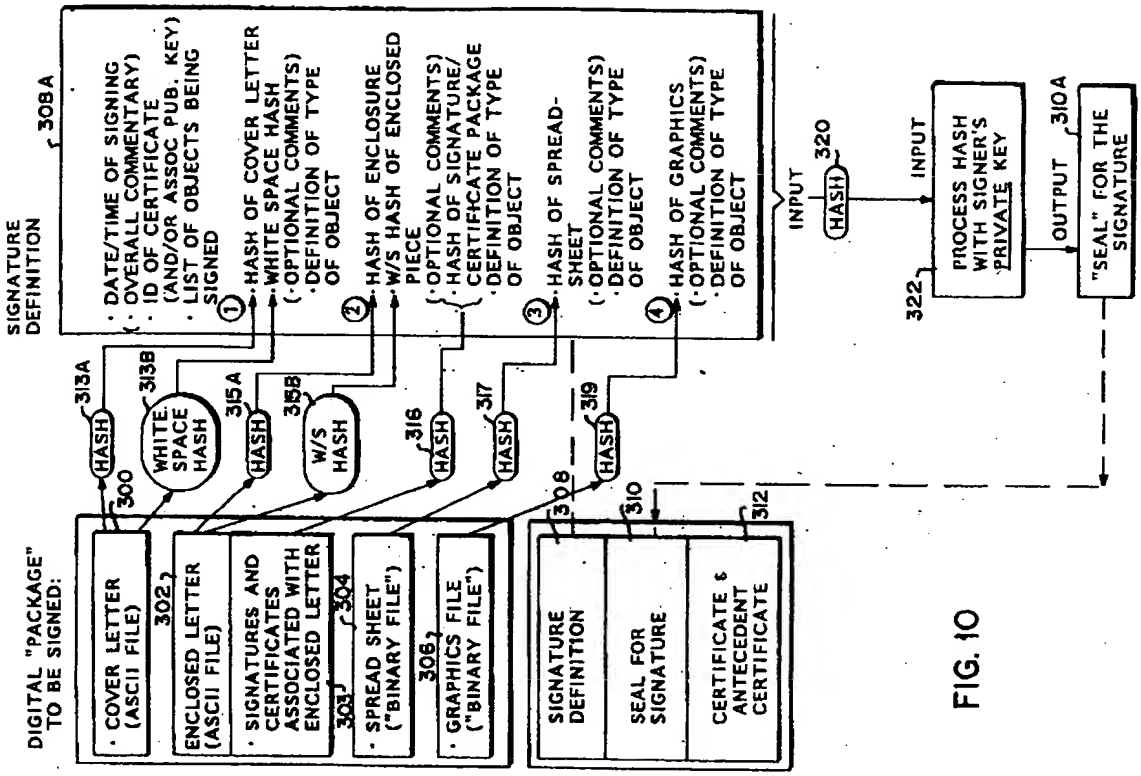

SIGNATURE DEFINITION
308A
· DATE/TIME OF SIGNING
· OVERALL COMMENTARY)
· ID OF CERTIFICATE (AND/OR ASSOC PUB. KEY)
· LIST OF OBJECTS BEING SIGNED
1 · HASH OF COVER LETTER
· WHITE SPACE HASH
(· OPTIONAL COMMENTS)
· DEFINITION OF TYPE OF OBJECT
2 · HASH OF ENCLOSURE
· W/S HASH OF ENCLOSED PIECE
(· OPTIONAL COMMENTS)
· HASH OF SIGNATURE/ CERTIFICATE PACKAGE
· DEFINITION OF TYPE OF OBJECT
3 · HASH OF SPREAD-SHEET
(· OPTIONAL COMMENTS)
· DEFINITION OF TYPE OF OBJECT
4 · HASH OF GRAPHICS
(· OPTIONAL COMMENTS)
· DEFINITION OF TYPE OF OBJECT
INPUT
320
HASH
INPUT
PROCESS HASH WITH SIGNER'S PRIVATE KEY
322
OUTPUT
310A
"SEAL" FOR THE SIGNATURE
313A
HASH
300
313B
WHITE SPACE HASH
315A
HASH
315B
W/S HASH
316
HASH
317
HASH
319
HASH
DIGITAL "PACKAGE" TO BE SIGNED:
· COVER LETTER (ASCII FILE)
302
ENCLOSED LETTER (ASCII FILE)
· SIGNATURES AND CERTIFICATES ASSOCIATED WITH ENCLOSED LETTER
304
303
· SPREAD SHEET ("BINARY FILE")
306
· GRAPHICS FILE ("BINARY FILE")
308
SIGNATURE DEFINITION
310
SEAL FOR SIGNATURE
312
CERTIFICATE & ANTECEDENT CERTIFICATE

FIG. 10

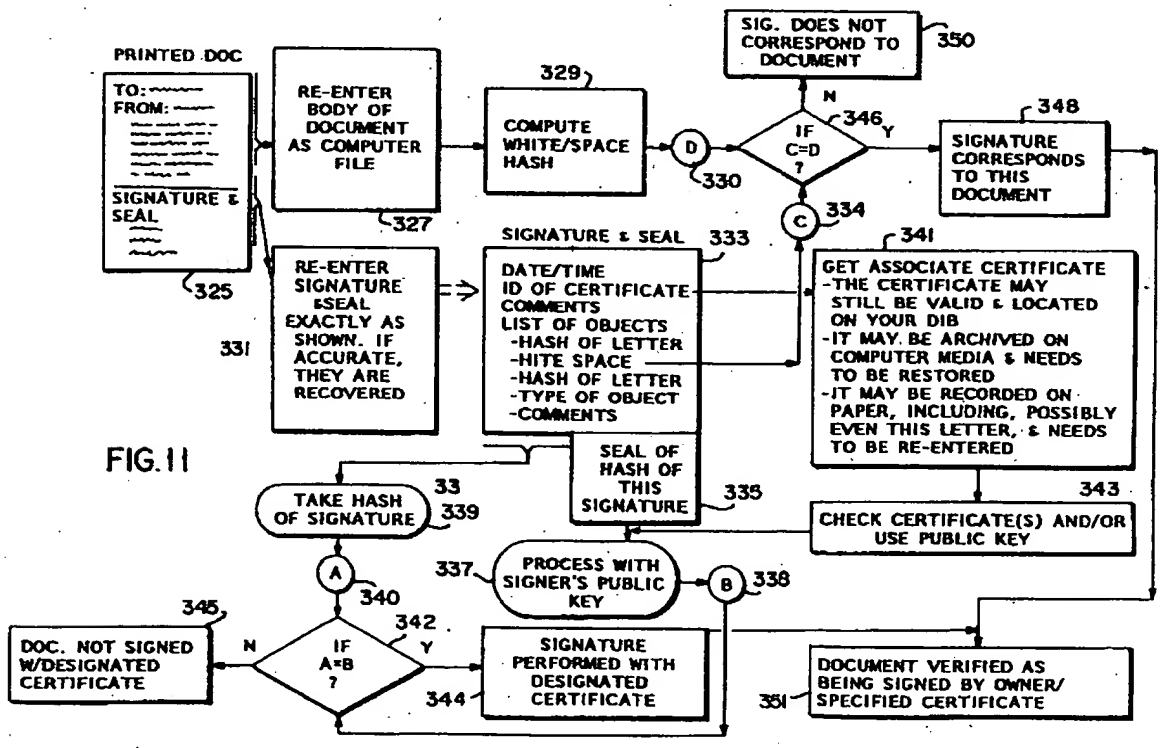

PRINTED DOC
TO:
FROM:
SIGNATURE & SEAL
325
RE-ENTER BODY OF DOCUMENT AS COMPUTER FILE
327
RE-ENTER SIGNATURE &SEAL EXACTLY AS SHOWN. IF ACCURATE, THEY ARE RECOVERED
331
329
COMPUTE WHITE/SPACE HASH
D
330
SIG. DOES NOT CORRESPOND TO DOCUMENT
350
N
IF C=D ?
346
Y
348
SIGNATURE CORRESPONDS TO THIS DOCUMENT
C
334
SIGNATURE & SEAL
333
DATE/TIME
ID OF CERTIFICATE
COMMENTS
LIST OF OBJECTS
-HASH OF LETTER
-HITE SPACE
-HASH OF LETTER
-TYPE OF OBJECT
-COMMENTS
341
GET ASSOCIATE CERTIFICATE
-THE CERTIFICATE MAY STILL BE VALID & LOCATED ON YOUR DIB
-IT MAY BE ARCHIVED ON COMPUTER MEDIA & NEEDS TO BE RESTORED
-IT MAY BE RECORDED ON PAPER, INCLUDING, POSSIBLY EVEN THIS LETTER, & NEEDS TO BE RE-ENTERED
SEAL OF HASH OF THIS SIGNATURE
335
343
CHECK CERTIFICATE(S) AND/OR USE PUBLIC KEY
TAKE HASH OF SIGNATURE
33
339
A
340
337
PROCESS WITH SIGNER'S PUBLIC KEY
B
338
345
DOC. NOT SIGNED W/DESIGNATED CERTIFICATE
N
IF A=B ?
342
Y
SIGNATURE PERFORMED WITH DESIGNATED CERTIFICATE
344
DOCUMENT VERIFIED AS BEING SIGNED BY OWNER/ SPECIFIED CERTIFICATE
351

FIG. 11

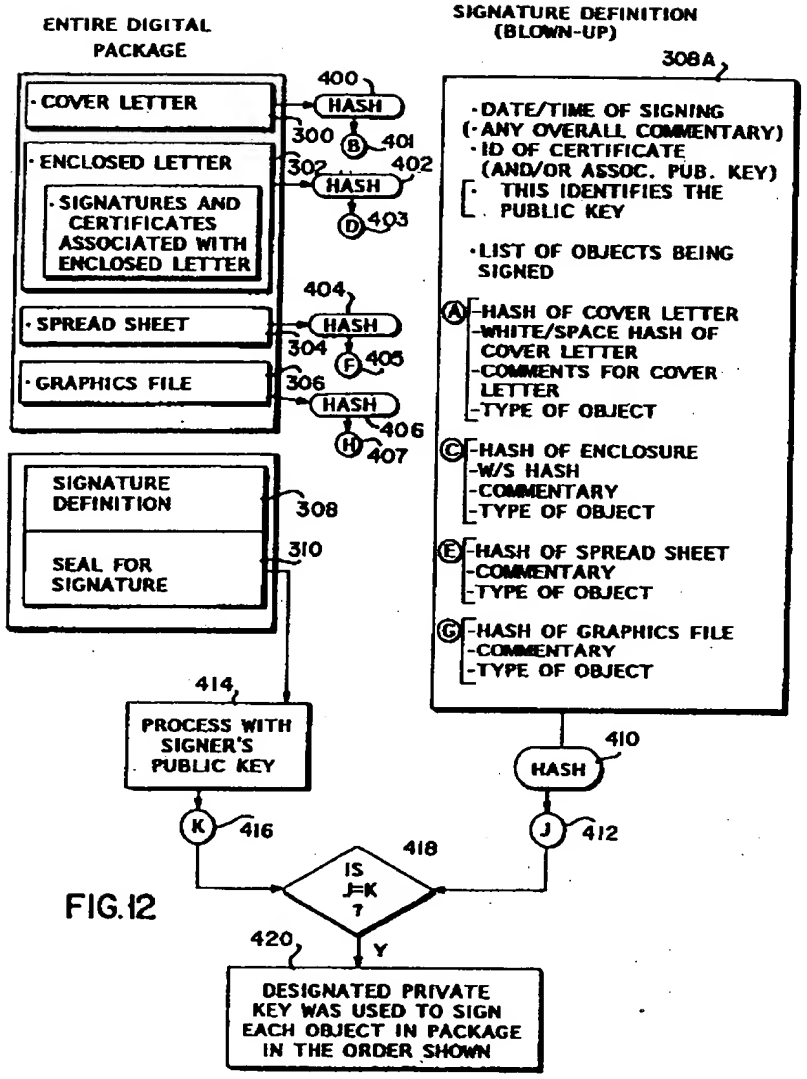

ENTIRE DIGITAL PACKAGE
SIGNATURE DEFINITION (BLOWN-UP)
308A
·COVER LETTER
·ENCLOSED LETTER
·SIGNATURES AND CERTIFICATES ASSOCIATED WITH ENCLOSED LETTER
·SPREAD SHEET
·GRAPHICS FILE
400
HASH
300
B
401
302
402
HASH
D
403
404
HASH
304
F
405
306
HASH
H
406
407
SIGNATURE DEFINITION
308
SEAL FOR SIGNATURE
310
·DATE/TIME OF SIGNING
(·ANY OVERALL COMMENTARY)
·ID OF CERTIFICATE (AND/OR ASSOC. PUB. KEY)
· THIS IDENTIFIES THE PUBLIC KEY
·LIST OF OBJECTS BEING SIGNED
A -HASH OF COVER LETTER
-WHITE/SPACE HASH OF COVER LETTER
-COMMENTS FOR COVER LETTER
-TYPE OF OBJECT
C -HASH OF ENCLOSURE
-W/S HASH
-COMMENTARY
-TYPE OF OBJECT
E -HASH OF SPREAD SHEET
-COMMENTARY
-TYPE OF OBJECT
G -HASH OF GRAPHICS FILE
-COMMENTARY
-TYPE OF OBJECT
414
PROCESS WITH SIGNER'S PUBLIC KEY
410
HASH
K
416
J
412
418
IS J=K ?
Y
420
DESIGNATED PRIVATE KEY WAS USED TO SIGN EACH OBJECT IN PACKAGE IN THE ORDER SHOWN

FIG.12